Regular subgroups of primitive permutation groups

Martin W. Liebeck
Department of Mathematics
Imperial College
London SW7 2BZ, UK

Cheryl E. Praeger
School of Mathematics and Statistics
University of Western Australia
Crawley, WA 6009, Australia

Jan Saxl
DPMMS
CMS, Wilberforce Road
Cambridge CB3 0WB, UK

Contents

Abstract

We address the classical problem of determining finite primitive permutation groups G with a regular subgroup B. The main theorem solves the problem completely under the assumption that G is almost simple. While there are many examples of regular subgroups of small degrees, the list is rather short (just four infinite families) if the degree is assumed to be large enough, for example at least 30!. Another result determines all primitive groups having a regular subgroup which is almost simple. This has an application to the theory of Cayley graphs of simple groups.

Received by the editor January 17, 2006.
2000 Mathematics Classification Numbers: 20B15, 05C25.
Key words and phrases: primitive permutation groups, simple groups, Cayley graphs, regular subgroups.
This paper forms part of a research project funded by an Australian Research Council Discovery Grant. Thanks are also due to Michael Giudici for his computational contributions to some of our proofs.

1 Introduction

The problem of investigating finite primitive permutation groups containing a regular subgroup goes back more than one hundred years. Burnside investigated first the groups of prime degree, and later showed that primitive groups containing a cycle of prime-power degree p^a are 2-transitive, except in the case $a = 1$. (A minor error in his proof was noticed and corrected independently by Peter Neumann and Wolfgang Knapp (see [27]).) Schur generalized this to primitive groups containing a regular cycle of any composite order. Burnside suggested that perhaps the existence of a regular p-subgroup B forced the primitive group to be 2-transitive, except in the case where B is elementary abelian. However, examples had already existed, due to W. Manning, of simply primitive groups in product action, with regular subgroups which are direct products of cyclic subgroups of equal orders (not necessarily prime – see [44, Theorem 25.7]). Wielandt investigated the problem extensively. Section 25 of his book [44] is devoted to the problem. To mark the contribution of Burnside, he coined the term B-group for any group B whose presence as a regular subgroup in a primitive group G forces G to be 2-transitive. He gave a number of classes of examples of groups which are B-groups [44, Section 25], some due to Bercov and Nagai. Wielandt also gave the first examples of non-abelian B-groups, proving that all dihedral groups are B-groups [44, Theorem 25.6].

With the classification of finite simple groups, one can make much further progress. By a result of Cameron, Neumann and Teague [8], if S denotes the set of natural numbers n for which there exists a primitive group of degree n other than A_n and S_n, then S has zero density in $\mathbb{N}$. Hence, for almost all integers n, all groups of order n are B-groups. Moreover, the 2-transitive permutation groups are known. It is natural to extend the problem and ask also for a list of all pairs (G, B) with G a primitive permutation group on a finite set Ω and B a regular subgroup. This is the problem we are considering here.

Our main method of analysis is to view this situation as a group factorization: for a pair (G, B) as above and a point α in the set Ω, the transitivity of B implies that $G = BG_\alpha$, and since B is regular on Ω we have in addition that $B \cap G_\alpha = 1$. The study of such factorizations was proposed by B. H. Neumann in his 1935 paper [38]. He called a factorization $G = AB$, where A, B are subgroups such that $A \cap B = 1$, a *general product*, and viewed it as a generalization of a direct product (without the requirement that A and B be normal). In [38], among other things, the equivalence was pointed out between general products $G = AB$ and transitive actions of G with point stabiliser A and regular subgroup B. According to Neumann [39, p. 65], general products were later called *Zappa-Rédei-Szép products* (see [41, 46]), and moreover they had already occurred in the book of de Séguier [10] in 1904. Independently of [38] and in the same year, G.A. Miller wrote about group factorizations in [37]. In particular he gave several examples of general products in which G is a finite alternating group A_n and A is a Mathieu group M_n with $8 \leq n \leq 12$, and noted that A_6 has no nontrivial expression as a general product.

In the more recent literature, general products have come to be better known as *exact factorizations*, and that is what we shall call them. Attempts to construct them synthetically have been made by P. W. Michor [36], both for groups and in the broader context of graded Lie algebras. (We thank Rudolph Zlabinger for drawing this work to our attention.) In contrast to this, our focus is analytical. We work from a given transitive (or primitive) permutation group G with point stabiliser A, and determine the existence or otherwise of a regular subgroup B.

Thus in our context the exact factorization $G = G_\alpha B$ is such that the subgroup G_α is maximal and core-free in G, since G acts primitively and faithfully on the set Ω. An outline reduction theorem for such exact factorizations, based on the Aschbacher-O'Nan-Scott theorem, was obtained in [35, Corollary 3]. The main cases left outstanding there were the case where G is almost simple and the case of G in product action. The former is addressed here and solved completely. The latter remains open and we hope to return to it in the future.

It should be mentioned that even for the types of primitive groups in [35, Corollary 3] where regular subgroups always exist (namely, diagonal, twisted wreath and affine types), the problem of determining *all* regular subgroups remains open; some interesting examples of regular subgroups exist, very different from the obvious ones (see, for example, [17] in the case of affine groups).

Our main result is a classification theorem for almost simple primitive permutation groups with a regular subgroup:

Theorem 1.1 *Let G be an almost simple primitive permutation group on a set Ω, with socle L. Suppose that G has a subgroup B which is regular on Ω. Then the possibilities for G, G_α $(\alpha \in \Omega)$ and B are given in Tables* 16.1 − 16.3 *at the end of the paper.*

Remarks (1) All entries in the tables give examples of regular subgroups, and this is verified for each entry as it arises in the proof. The fourth column of each table gives the number of possibilities for B up to conjugacy (except for Table 16.2, where this information is rather clear). Some of the details concerning these numbers were verified by Michael Giudici, using Magma [6]. More information about the sporadic group examples in Table 16.3 can be found in [15].

(2) Some related results on regular subgroups have been obtained independently by other researchers. Wiegold and Williamson [43] found all exact factorizations of alternating and symmetric groups. Recent papers of Jones and Li classify primitive permutation groups with regular cyclic subgroups [21], regular abelian subgroups [28], and regular dihedral subgroups [29]. Li and Seress [30, Theorem 1.2] handle the special case where the degree $|\Omega|$ is square-free and the regular subgroup B lies in L. Regular subgroups of two sporadic groups ($HS.2$ and $J_2.2$) have been found in [18, 22], and all factorizations of sporadic groups are determined in [15]. Finally, some families of almost simple primitive groups have been dealt with independently by Baumeister in [4, 5]. In particular she handles unitary groups and 8-dimensional orthogonal groups of plus-type; however, for completeness we include our own proofs for these groups.

We remark also on a couple of features of our proof of Theorem 1.1, which may be of independent interest. The first involves the classification of antiflag transitive linear groups, presented in Section 3; this updates and slightly generalizes the famous work of Cameron and Kantor [7] on such groups. The second is the work in Section 4, which contains some detailed results determining the subgroups of classical groups which are transitive on various types of subspaces.

Despite the fairly long lists of regular subgroups in Tables 16.1 - 16.3, there are essentially only four infinite families:

Corollary 1.2 *Let G be an almost simple primitive permutation group of degree n, with $G \not\geq A_n$ and $n > 3 \cdot 29!$, and suppose that G has a regular subgroup B. Then one of the following holds:*

(i) *B is metacyclic, of order $(q^m - 1)/(q - 1)$ for some prime power q;*

(ii) *B is a subgroup of odd order $q(q - 1)/2$ in $A\Gamma L_1(q)$ for some prime power $q \equiv 3 \bmod 4$;*

(iii) *$B = A_{p-2}$, S_{p-2} (p prime), or $A_{p-2} \times 2$ (p prime, $p \equiv 1 \bmod 4$);*

(iv) *$B = A_{p^2-2}$ (p prime, $p \equiv 3 \bmod 4$).*

Table 1: Almost simple primitive groups sharing a common regular subgroup

inclusions $\mathrm{soc}(G) < \mathrm{soc}(H)$	common regular subgroup B
$A_p < A_{p+1}$ (p prime)	S_{p-2} or $A_{p-2} \times 2$
$A_{10} < A_{11} < A_{12}$	A_7
$L_2(11) < M_{11} < A_{11}$	11 or 11.5
$L_2(11) < M_{12}$	[12]
$L_2(23) < M_{24}$	[24]
$M_{23} < A_{23}$	23.11
$M_{23} < M_{24}$	$L_3(4).2$ or $2^4.A_7$
$A_7 < A_8 < \{A_9,\, Sp_6(2)\} < \Omega_8^+(2) < Sp_8(2)$	S_5
$Sp_4(4).2 < Sp_8(2)$	S_5
$Sp_6(2) < \Omega_8^+(2)$	$2^4.A_5$
$Sp_6(4).2 < \Omega_8^+(4).2$	$L_2(16).4$

Corollary 1.2 is an immediate consequence of Theorem 1.1.

Theorem 1.1 throws up some interesting containments between primitive subgroups of S_n which share a common regular subgroup. In the next result we classify all such containments for which the smaller group is almost simple. The proof can be found at the end of Section 15.

Corollary 1.3 *Let G be an almost simple primitive permutation group of degree n, not containing A_n, such that G contains a regular subgroup B. Then one of the following holds:*

(i) *$N_{S_n}(G)$ is maximal in A_n or S_n;*

(ii) *$n = 8$, $G = L_2(7) < AGL_3(2)$, sharing a regular subgroup $B = D_8$;*

(iii) *there is an almost simple group H such that $G < H < S_n$ and* $\mathrm{soc}(G) < \mathrm{soc}(H)$*; the inclusion* $\mathrm{soc}(G) < \mathrm{soc}(H)$ *and the common regular subgroup B are as in one of the lines of Table* 1*, and the actions of G, H can be read off from the tables in Section* 16.

It can be seen from Table 1 that there are no fewer than seven primitive groups of degree 120 sharing a common regular subgroup (namely S_5). Figure 1 gives the lattice of containments among these groups.

$$\begin{tikzcd}
 & Sp_8(2) & & \\
Sp_4(4).2 \arrow[ur] & & O_8^+(2) \arrow[ul] & \\
 & A_9 \arrow[ur] & & Sp_6(2) \arrow[ul] \\
S_7 \arrow[ur] & & S_8 \arrow[ur] &
\end{tikzcd}$$

Figure 1: Groups of degree 120 sharing a regular subgroup S_5

Some of the work discussed above was concerned with deciding whether certain classes of groups are B-groups. In particular, the papers [21, 28, 29] of Jones and Li deal with the cases of cyclic and dihedral regular subgroups. At the opposite end, we classify in Theorem 1.4 below the primitive permutation groups with regular almost simple subgroups. Burnside already knew examples of simply primitive permutation groups with regular simple subgroups. We discuss these next.

Any group T induces a regular permutation group acting on itself by right multiplication; $x \in T$ maps $y \mapsto yx$ $(y \in T)$. Identifying T with this regular subgroup of $\mathrm{Sym}(T)$, we define the *holomorph* of T as the normalizer of T in $\mathrm{Sym}(T)$, denoted $\mathrm{Hol}(T)$. This group contains the centraliser $C = C_{\mathrm{Sym}(T)}(T)$ which is isomorphic to T, where each $x \in T$ corresponds to the element c_x of C that maps $y \mapsto x^{-1}y$ $(y \in T)$. In general the holomorph is the semidirect product $\mathrm{Hol}(T) = T \cdot \mathrm{Aut}(T)$ with $\mathrm{Aut}(T)$ acting naturally, both T and C are regular normal subgroups, and $C \cap T = Z(T)$. Moreover the permutation $\sigma : y \mapsto y^{-1}$ $(y \in T)$ normalizes $\mathrm{Hol}(T)$, interchanges T and C $(\sigma : x \leftrightarrow c_x$ for each $x \in T)$, and centralizes $\mathrm{Aut}(T)$. In the case where T is a non-abelian simple group, the permutation group $\langle \mathrm{Hol}(T), \sigma \rangle \leq \mathrm{Sym}(T)$ is denoted by $D(2, T)$. This is a primitive permutation group of diagonal type, and $C \times T$ is its unique minimal normal subgroup.

The groups $D(2, T)$ form an important family of finite primitive groups having simple regular subgroups, as demonstrated by the following theorem. This theorem also shows that there are infinitely many finite primitive groups with an almost simple regular subgroup that is not simple.

Theorem 1.4 *Let G be a primitive permutation group on a finite set Ω of size n, and suppose that G has a subgroup B which is almost simple and acts regularly on Ω. Then one of the following holds:*

(i) *$G = A_n$ or S_n, and $|B| = n$;*

(ii) *there is a non-abelian simple group T such that $G \leq D(2, T)$ with $\mathrm{soc}(G) = T^2$, and $B \cong T$;*

(iii) *G is almost simple, and B and G are as in Table 2 below.*

In particular, if B is not simple, then G is almost simple, and either G contains A_n, or B, G are as in the lower part of Table 2.

The proof of this theorem appears in Section 15. An immediate consequence is the classification of the almost simple B-groups, recorded in Corollary 1.5 below. In contrast with the situation for simple groups, the non-simple almost simple groups are usually B-groups:

Corollary 1.5 *If G is an almost simple group, then G is a B-group if and only if both the following conditions hold:*

(i) *G is not simple;*

(ii) *$G \neq S_{p-2}$ (p prime), $L_2(16).4$, or $L_3(4).2$.*

Theorem 1.4 has another immediate consequence, concerning the structure of Cayley graphs of finite simple groups. For any group G and subset $S \subseteq G \setminus \{1\}$, the *Cayley digraph* $\mathrm{Cay}(G, S)$ for G relative to S is the digraph with vertex set G and with an edge from x to y whenever $xy^{-1} \in S$. If $S^{-1} := \{x^{-1} | x \in S\}$ is equal to S, then the adjacency relation is symmetric, so the Cayley digraph can be regarded as an undirected graph, called a Cayley graph. In particular, if $S = G \setminus \{1\}$, then $\mathrm{Cay}(G, S)$ is a complete graph on $n = |G|$ vertices with automorphism group S_n. In all cases the group G, acting by right multiplication, is admitted as a subgroup of automorphisms which is regular on the set of vertices. Moreover, $\mathrm{Cay}(G, S)$ is connected if and only if S generates G.

A general analysis was made in [13] of the possible structures of the automorphism groups of $\mathrm{Cay}(T, S)$ for finite nonabelian simple groups T. As a consequence of [13, Theorem 1.1], for generating sets S with $S = S^{-1}$ and $S \neq T \setminus \{1\}$, one does not expect the automorphism group of $\mathrm{Cay}(T, S)$ to be vertex-primitive, a notable exceptional case being that in which S is a union of T-conjugacy classes; in the latter case the automorphism group has socle T^2, and is a primitive subgroup of $D(2, T)$. Restating Theorem 1.4 in the language of Cayley graphs, in the case where $B = T$ is simple, gives a classification of all vertex-primitive Cayley digraphs of finite nonabelian simple groups. If the automorphism group contains A_n, where $|T| = n$, or contains $L_2(59)$ with $T = A_5$, then the automorphism group is 2-transitive

Table 2: Almost simple regular subgroups

B	$\mathrm{soc}(G)$	$(\mathrm{soc}(G))_\alpha$ $(\alpha \in \Omega)$	Remark
A_5	$L_2(59)$	$59 \cdot 29$	
A_7	A_{11}, A_{12}	M_{11}, M_{12} (resp.)	
A_{p^2-2} (p prime $\equiv 3 \bmod 4$)	A_{p^2+1}	$L_2(p^2).2$	
S_{p-2} ($p \geq 7$ prime)	$A_p,\ A_{p+1}$	$p.\frac{p-1}{2},\ L_2(p)$ (resp.)	
S_5	A_9	$L_2(8).3$	
	$Sp_4(4)$	$L_2(16).2$	$G = L.2$
	$Sp_6(2)$	$G_2(2)$	
	$\Omega_8^+(2)$	$\Omega_7(2)$	
	$Sp_8(2)$	$O_8^-(2)$	
$L_2(16).4$	$Sp_6(4),\ \Omega_8^+(4)$	$G_2(4),\ \Omega_7(4)$ (resp.)	$G \geq L.2$
$L_3(4).2$	$M_{23},\ M_{24}$	$23.11,\ L_2(23)$ (resp.)	

on vertices, implying that the generating set $S = T \setminus \{1\}$. If we assume this is not so, then these cases of Theorem 1.4 do not arise in the Cayley graph setting. Thus we obtain Theorem 1.6 below as a consequence of Theorem 1.4. This completes the results of [13] for vertex-primitive Cayley digraphs.

Theorem 1.6 *Let T be a simple group, and suppose that T has a generating set $S = S^{-1}$ such that the Cayley graph* $\mathrm{Cay}(T, S)$ *has automorphism group acting primitively on vertices, and is not a complete graph. Then one of the following holds:*

(i) *S is a union of conjugacy classes of T ;*

(ii) *$T = A_{p^2-2}$, with p prime, $p \equiv 3$ mod 4.*

Remark In both (i) and (ii) there are examples of vertex primitive, non-complete Cayley graphs. This was discussed in the preamble to the theorem for case (i). For case (ii), observe from Table 16.2 that the group A_{p^2+1} acting primitively on the cosets of a maximal subgroup $L_2(p^2).2$ possesses a regular subgroup A_{p^2-2}; hence any orbital graph for this A_{p^2+1} is necessarily a Cayley graph for the regular subgroup A_{p^2-2}. The smallest case is $p = 3$, $T = A_7$.

Cayley graphs for these groups have arisen also as exceptional examples in a different context. In [45] a study of cubic, s-arc transitive, Cayley graphs for finite non-abelian simple groups revealed that there are exactly two such graphs for which $s > 2$, and these are both 5-arc transitive Cayley graphs for A_{47} with automorphism group A_{48}. However, neither of these graphs is vertex-primitive.

There is one further application that we should mention. Exact factorizations of finite groups can be used to obtain semisimple Hopf algebras. The construction, using bicrossproducts, goes back to Kac and Takeuchi, and is outlined in the paper [12]. In that paper, the exact factorization $M_{24} = L_2(23)(2^4A_7)$ is used to construct a biperfect Hopf algebra of dimension $|M_{24}|$. (A Hopf algebra H is biperfect if neither H nor H^* has any non-trivial 1-dimensional representations.) It is not known whether there exist biperfect Hopf algebras of smaller dimension. For the bicrossproduct construction, one needs an exact factorization of a group G with both factors perfect and self-normalizing in G, see [12].

The layout is as follows. After some preliminaries in Section 2, we present in Section 3 the classification of antiflag transitive linear groups, remarked upon earlier. Section 4 contains some detailed results determining the subgroups of classical groups which are transitive on various types of subspaces. Sections 5 – 11 contain the proof of Theorem 1.1 for the classical groups, which is by far the bulk of the proof; the proofs for the exceptional groups of Lie type, the alternating groups and the sporadic groups are given in the following much shorter Sections 12 – 14. Section 15 contains the proofs of Theorem 1.3 and Corollary 1.2, and finally Section 16 comprises Tables 16.1 – 16.3, referred to in the statement of Theorem 1.1.

2 Preliminaries

In this section we collect various results from the literature which will be needed in our proofs.

Notation First we introduce some notation for certain types of subgroups in classical groups. Let G be a finite almost simple classical group with socle L and associated vector space V. As usual, denote by P_i the parabolic subgroup of G obtained by deleting the ith node of the standard Dynkin diagram; so P_i is the stabilizer of a totally singular i-dimensional subspace of V, except when $L = P\Omega^+_{2m}(q)$ and $i = m-1$. In this last case there are two L-orbits on totally singular m-spaces, P_{m-1} and P_m being the stabilizers of representatives of the different orbits. Also P_{ij} denotes the intersection of two parabolic subgroups P_i and P_j sharing a common Borel subgroup.

When $L = L_n(q)$, denote by $N_{1,n-1}$ the stabilizer of a pair of complementary subspaces of V of dimensions $1, n-1$.

When $L = Sp_n(q)$ with q even, write O^ϵ for the normalizer in G of the natural subgroup $O^\epsilon_n(q)$ of L.

Now assume G is unitary, symplectic or orthogonal, and let W be a nonsingular subspace of V of dimension i. We denote the stabilizer G_W of W in G by N_i, N_i^+ or N_i^- as follows:

$G_W = N_i$, if G is unitary or symplectic, or if $L = P\Omega^\pm_{2m}(q)$ and i is odd;

$G_W = N_i^\epsilon$ ($\epsilon = \pm$), if i is even, G is orthogonal and W has type O^ϵ;

$G_W = N_i^\epsilon$ ($\epsilon = \pm$), if i is odd, $L = P\Omega_{2m+1}(q)$ (q odd) and $W^\perp$ has type O^ϵ.

For a classical subgroup H of G, we will sometimes write $P_i(H), N_i(H)$, etc. for the relevant parabolic subgroup P_i or nonsingular subspace stabiliser N_i in H. Also q will always denote a power $q = p^a$ of a prime p, and when we write $\log q$ we will mean $\log_p q = a$. Finally for such a $q = p^a$, we denote by q_n a *primitive prime divisor* of $q^n - 1$, that is, a prime which divides $p^{an} - 1$ but not $p^i - 1$ for $1 \leq i < an$. By [47], such a prime exists except in the cases where $(p, an) = (2, 6)$ or $an = 2$, $p + 1 = 2^b$.

The first two lemmas of this section concern the classification of involution classes in symplectic and orthogonal groups in characteristic 2, and are taken from [2, Sections 7,8].

Let V be a vector space of even dimension $2m$ over a finite field of characteristic 2, and let $(\ ,\ )$ be a non-degenerate symplectic form on V with corresponding symplectic group $Sp(V)$. For an involution $t \in Sp(V)$, define

$$V(t) = \{v \in V \ : \ (v, t(v)) = 0\}.$$

The Jordan form of t is (J_2^l, J_1^{2m-2l}) for some l, where J_i denotes a Jordan block of size i.

Lemma 2.1 *Let V be a vector space of dimension $2m$ over a field of characteristic 2. The conjugacy classes of involutions in $Sp(V)$ have representatives*

$$\begin{array}{l} a_l \ (l \ \textit{even}, 2 \leq l \leq m), \\ b_l \ (l \ \textit{odd}, 1 \leq l \leq m), \\ c_l \ (l \ \textit{even}, 2 \leq l \leq m), \end{array}$$

where a_l, b_l, c_l all have Jordan form (J_2^l, J_1^{2m-2l}), and

$$V(a_l) = V, \ V(b_l) \neq V, \ V(c_l) \neq V.$$

Now assume $m \geq 2$ and let $O^\epsilon(V)$ be an orthogonal group on V of type $\epsilon \in \{+, -\}$ lying in $Sp(V)$, with commutator subgroup $\Omega^\epsilon(V)$.

Lemma 2.2 (i) *Involutions in $O^\epsilon(V)$ are conjugate in $O^\epsilon(V)$ if and only if they are conjugate in $Sp(V)$.*

(ii) *a_l lies in $\Omega^+(V)$ for all l, and in $\Omega^-(V)$ for all l except for $l = m$ (m even); for m even, a_m does not lie in $O^-(V)$.*

(iii) *b_l lies in $O^+(V)$ and in $O^-(V)$, but not in $\Omega^\epsilon(V)$.*

(iv) *c_l lies in $\Omega^+(V)$ and in $\Omega^-(V)$.*

Corollary 2.3 *If $\epsilon = +$, or if $\epsilon = -$ and m is odd, then every involution class representative a_l, b_l, c_l lies in $O^\epsilon(V)$. If $\epsilon = -$ and m is even, then every involution class representative except a_m lies in $O^\epsilon(V)$.*

We shall also need some information about unipotent elements of symplectic and orthogonal groups in odd characteristic, taken from [42, pp.36-39].

Lemma 2.4 *Let q be a power of an odd prime, and let u be a unipotent element of $GL_n(q)$ with Jordan form $(J_1^{n_1}, J_2^{n_2}, \ldots)$. Then the following hold.*

(i) *u is similar to an element of $Sp_n(q)$ if and only if n_i is even for each odd i.*

(ii) *u is similar to an element of some orthogonal group $O_n(q)$ if and only if n_i is even for each even i.*

(iii) *Assume that n is even, and also that n_i is even for each even i. If $n_j > 0$ for some odd j, then u is similar to elements of both $O_n^+(q)$ and $O_n^-(q)$. Otherwise, u is similar to an element of $O_n^+(q)$ but not of $O_n^-(q)$.*

The next lemma gives some basic information on the representations of $G = SL_2(q)$ (q even) in characteristic 2. If V is an $\mathbb{F}_qG$-module, denote by $V^{(2^i)}$ the $\mathbb{F}_qG$-module V with G-action twisted by a Frobenius 2^i-power automorphism (i.e. with action $v * g = vg^{(2^i)}$ for $v \in V, g \in G$).

Lemma 2.5 *Let $G = SL_2(2^e)$ with $e \geq 2$, and let $W = V_2(2^e)$ be the natural 2-dimensional module for G. Write $F = \mathbb{F}_{2^e}$, and let V be an irreducible FG-module.*

(i) *Then $V \cong W^{(2^{i_1})} \otimes \cdots \otimes W^{(2^{i_k})}$ for some $i_1, \ldots, i_k$ satisfying $0 \leq i_1 < \cdots < i_k < e$.*

(ii) *If $H^1(G, V) \neq 0$ then $V \cong W^{(2^i)}$ for some i, in which case $H^1(G, V)$ has dimension 1.*

Proof Part (i) is immediate from Steinberg's tensor product theorem, and (ii) follows from [1, 4.5]. ■

We conclude this section with a lemma (essentially the main theorem of [34]) that relates our exact factorization $G = BG_\alpha$, with G almost simple and G_α maximal, with a maximal factorization of G or a closely related subgroup. For an almost simple group G with socle L, and a subgroup A of G, we write $A \max^- G$ to mean that A is maximal among core-free subgroups of G (so that all overgroups of A in G contain L), and we write $A \max^+ G$ to mean that A is both core-free and maximal in G. Note that, for any subgroup B of G it is always possible to choose an overgroup B^*

of B such that $B^* \max^- G$. An expression $G = AB$ is called a *maximal factorization* if both $A \max^+ G$ and $B \max^+ G$, and a $\max^-$ *factorization* if both $A \max^- G$ and $B \max^- G$.

In the next result, notation in the table is as defined at the beginning of this section.

Lemma 2.6 *Let G be a finite almost simple group with socle L, and let $G = AB$, where $A \max^+ G$. Let B^* satisfy $B \le B^* \le G$ and $B^* \max^- G$, and set $G^* := B^* L$, $A^* = A \cap G^*$.*

Then $G^* = A^* B^*$, and either this is a maximal factorization (determined by [33]), or $L, A \cap L, B^* \cap L$ are as in one of the lines of the following table.

L	$A \cap L$	$B^* \cap L$
$L_{2m}(q)$ (*with* $(q-1, m) \neq 1$)	$N_{1,2m-1}$	$N_L(PSp_{2m}(q))$
$P\Omega^+_{2m}(q)$ (q *odd*, m *odd*)	$N_L(GL_m(q)/\langle -1 \rangle)$	N_1
$P\Omega^+_8(3)$	$\Omega_7(3)$	$\Omega^+_6(3).2$
$P\Omega^+_8(3)$	$\Omega^+_8(2)$	P_{ij} ($i, j \in \{1,3,4\}$)
$P\Omega^+_8(3)$	$2^6.A_8$	P_i ($i \in \{1,3,4\}$)
M_{12}	A_5	M_{11}

Proof Since $A \max^+ G$, we have $G = AL$. Moreover, $G = AB^*$ is a $\max^-$ factorization. Now the result follows directly from [34, Theorem]. ∎

3 Transitive and antiflag transitive linear groups

Let $V = V_n(q)$ be a vector space of dimension n over $\mathbb{F}_q$. An *antiflag* of V is an unordered pair $\{\alpha, H\}$, where α is a 1-space in V and H is a hyperplane not containing α. A subgroup of $\Gamma L_n(q)$ is *antiflag transitive* if it is transitive on the set of all antiflags. An important role in our proofs is played by the classification of all antiflag transitive subgroups of $\Gamma L_n(q)$, achieved by Cameron and Kantor in [7]. However, a few errors in their conclusion have come to light over the years (see for example [33, Proposition B, p.45]). The source of the error is [7, p.401, line 2], and it can presumably be easily corrected, though such a correction has not appeared in the literature. Moreover, for our purposes we require a slightly more general version of their result, allowing the possibility that the antiflag transitive subgroup contains an element in the coset of a graph automorphism ι of $L_n(q)$ (where ι is the inverse-transpose automorphism if $n \ge 3$, and is the identity if $n = 2$). Here we extend the definition of antiflag transitive groups to include subgroups of $\Gamma L_n(q).\langle\iota\rangle$, which is justified since ι acts on the set of antiflags.

In view of all this, we include in this section a full proof of this slightly generalised form of the classification of antiflag transitive groups. Note however that our proof uses the classification of finite simple groups, whereas [7] does not.

We shall need the following well known result of Hering, classifying the subgroups of $\Gamma L_n(q)$ which are transitive on 1-spaces - see [31, Appendix] for a short proof of this result.

Lemma 3.1 *Let $H \le \Gamma L_n(q)$ be transitive on the set of 1-spaces of $V_n(q)$. Then one of the following holds:*

(i) $H \triangleright SL_a(q^b)\,(ab = n, a > 1)$, $Sp_a(q^b)\,(ab = n, a$ *even*$)$ *or* $G_2(q^b)'\,(6b = n, q$ *even*$)$*;*

(ii) $H \le \Gamma L_1(q^n)$*;*

(iii) *one of:*

$$\begin{array}{l} n = 2,\ q \in \{5, 7, 11, 23\}\ :\ H \triangleright Q_8 \\ n = 2,\ q \in \{9, 11, 19, 29, 59\}\ :\ H \triangleright SL_2(5) \\ n = 4,\ q = 2\ :\ H = A_6 \text{ or } A_7 \\ n = 4,\ q = 3\ :\ 2^{1+4} \triangleleft H \le 2^{1+4}.S_5 \text{ or } H \triangleright SL_2(5) \\ n = 6,\ q = 3\ :\ H = SL_2(13). \end{array}$$

Now we are ready to prove the main result of this section, classifying the antiflag transitive subgroups of $\mathrm{Aut}(L_n(q))$.

Theorem 3.2 *Suppose that $H \le \Gamma L_n(q).\langle\iota\rangle$ is antiflag transitive.Then one of the following holds:*

(i) $H \triangleright SL_n(q), Sp_n(q)\,(n$ *even*$)$ *or* $G_2(q)'\,(n = 6, q$ *even*$)$*;*

(ii) $q = 2$ *or* 4*,* $n \ge 4$ *is even, and* $H \triangleright SL_{n/2}(q^2), Sp_{n/2}(q^2)$ *or* $G_2(q^2)\,(n = 12)$*; moreover H contains a full group of field automorphisms in each case;*

(iii) $n = 4, q = 2$ *and* $H = A_6$ *or* A_7*;*

(iv) $n = 2, q = 4$ *and* $H = \Gamma L_1(q^2) = 15.4$.

Conversely, each of the possibilities in (i)-(iv) *does give rise to examples of antiflag transitive subgroups.*

Proof Let $H^0 = H \cap \Gamma L_n(q)$. Then H^0 has t orbits ($t \le 2$) of equal size on the set of antiflags, which has size $q^{n-1}.\frac{q^n-1}{q-1}$. If $t = 2$ the two H_0-orbits are interchanged by an element of the coset $\iota\Gamma L_n(q)$ normalizing H^0 (where ι is as defined above); in particular we have $n \geq 3$ when $t = 2$. By [33, 4.2.1], H^0 is transitive on $P_1(V)$, the set of 1-spaces of $V = V_n(q)$.

Fix a point $\alpha = \langle v \rangle \in P_1(V)$. For a hyperplane W not containing α we have $H_{\alpha,W} = (H^0)_{\alpha,W}$. If $H_{\{\alpha,W\}}$ interchanges α and W then $t = 1$, H^0 is transitive on antiflags, and $(H^0)_\alpha$ is transitive on the hyperplanes W not containing α. Alternatively if $H_{\{\alpha,W\}} = H_{\alpha,W}$, then $t = 2$ and $(H^0)_\alpha$ has 2 orbits of equal size on the hyperplanes W not containing α, of which there are q^{n-1}. In particular it follows that if $t = 2$ then q is even.

Being transitive on $P_1(V)$, the possibilities for H^0 are given by Lemma 3.1. The groups $A_6, A_7 < L_4(2)$ are listed in the conclusion. The other possibilities for H^0 in 3.1(iii) have q odd; hence if H^0 were one of them, then t would be 1 and $|H^0|$ would be divisible by q^{n-1}, which is not the case.

Hence we may assume that either $H^0 \triangleright SL_a(q^b), Sp_a(q^b)$ $(ab = n, a \geq 2)$ or $G_2(q^b)'$ $(6b = n)$, or $H^0 \leq \Gamma L_1(q^b)$ $(b = n)$.

Write $F = \mathbb{F}_q$ and $K = \mathbb{F}_{q^b}$, so that $\alpha = Fv$. Clearly $H^0_\alpha = H^0_{Fv}$ fixes Kv, a 1-space over $\mathbb{F}_{q^b}$, and, writing $J = (H^0_\alpha)^{Kv}$, we have $J \leq \Gamma L_1(q^b)$. Moreover, J fixes $\alpha = Fv$, so cannot contain any scalars in $K^* \backslash F^*$, and therefore $|J\mathbb{F}_q^*/\mathbb{F}_q^*|$ divides $b \log_p q$.

Any F-hyperplane W not containing α intersects Kv in an F-space of dimension $b-1$. Consequently J has at most t orbits on such $(b-1)$-spaces, of which there are q^{b-1}. If $t = 1$ this implies that q^{b-1} divides $b \log q$, hence either $b = 1$ or $b = 2$, $q = 2$ or 4. Both these possibilities are listed in the conclusion. (Note that $\Gamma L_1(4) = SL_2(2)$ and occurs in (i).)

Now assume that $t = 2$. Then q is even, and we have

$$q^{b-1} \leq 2b \log q. \tag{1}$$

Hence the possibilities for b, q are

$$\begin{aligned} &b = 1 \\ &b = 2,\ q = 2, 4, 8 \text{ or } 16 \\ &b = 3,\ q = 2 \\ &b = 4,\ q = 2. \end{aligned}$$

The cases $b = 1$ and $b = 2,\ q = 2, 4$ are listed in the conclusion. It remains to exclude the other cases.

Consider the case where $H^0 \leq \Gamma L_1(q^b)$ $(b = n)$. Since $t = 2$ we must have $\iota \neq 1$, hence $n = b \geq 3$ and $q = 2$. If $n = 3$ then H^0 has odd order so H cannot be transitive on the 28 antiflags. And if $n = 4$ then

$|\Gamma L_1(2^4)| = 2^3.3.5$ is equal to the number of antiflags, so $H = 3.2 \times 5.4 < L_4(2).2 \cong S_8$; however H then contains a conjugate of an involution in the antiflag stabilizer $L_3(2).2$, so cannot be antiflag transitive.

Assume from now on that $H^0 \rhd SL_a(q^b), Sp_a(q^b)$ $(ab = n, a \geq 2)$ or $G_2(q^b)'$ $(6b = n)$. Consider first the case where $b = 2, q = 16$. Here equality holds in (1), so we must have

$$H^0 = \Gamma L_a(q^2),\ \Gamma Sp_a(q^2) \text{ or } \Gamma G_2(q^2) < \Gamma L_{2a}(q) = \Gamma L_n(q).$$

By assumption, H^0 is normalized by an element in the coset $\iota\Gamma L_{2a}(q)$. When $H^0 = \Gamma L_a(q^2)$ or $\Gamma G_2(q^2)$, it is clear from the structure of $\mathrm{Aut}(H^0)$ that any group of the form $H^0.2$ contains an outer involution; and the same holds when $H^0 = \Gamma Sp_a(q^2)$, noting that for $a = 4$, the graph automorphism of $(H^0)'$ is not induced (indeed, $(H^0)'$ is centralized by an element of $\iota\Gamma L_{2a}(q)$).

We conclude that H^0 is normalized by an involution $\tau \in \iota\Gamma L_{2a}(q)$. By [2, 19.8], there are two $GL_{2a}(q)$-classes of involutions in this coset, with representatives ι (the inverse-transpose map) and ιJ, where

$$J = \begin{pmatrix} 0 & I_a \\ I_a & 0 \end{pmatrix}.$$

We have $C_{SL_{2a}(q)}(\iota J) = Sp_{2a}(q)$, while $C_{SL_{2a}(q)}(\iota)$ is the centralizer of a long root element in $Sp_{2a}(q)$, hence in particular lies in a parabolic subgroup of $Sp_{2a}(q)$.

Of the two involution class representatives above, ι clearly normalizes an antiflag stabilizer, while ιJ does not (it sends $G_{\langle v\rangle}$ to $G_{v^\perp}$, where $G = GL_{2a}(q)$ and the perp is relative to the symplectic form defined by J).

We aim to show that H^0 is normalized by a conjugate of ι. This will give a contradiction, since by assumption, the 2 orbits of H^0 on antiflags are interchanged by an element of the coset $\iota\Gamma L_n(q)$ normalizing H^0; this clearly cannot be the case for a conjugate of ι, since ι fixes an antiflag.

Consider the case where $(H^0)' = SL_a(q^2)$. Write $L = (H^0)'$. Suppose a is even. Then the coset $L\tau$ contains an involution, which we may as well label as τ, such that $C_L(\tau) = Sp_a(q^2)$. This is not contained in the centralizer of ι, and hence τ must be $GL_{2a}(q)$-conjugate to ιJ. Replacing H by a conjugate, we may take $\tau = \iota J$.

Now $C_{SL_{2a}(q)}(\iota J) = Sp_{2a}(q)$, the symplectic group fixing the form $(\ ,\ )$ defined by J. Clearly J itself lies in this centralizer, has Jordan form J_2^a, and satsifies $(v, vJ) \neq 0$ for some $v \in V$. By Lemma 2.1, the subgroup

$C_L(\tau) = Sp_a(q^2)$ contains an involution t which is $Sp_{2a}(q)$-conjugate to J. (Recall that a is even.) Then $t\iota J$ is $Sp_{2a}(q)$-conjugate to $J\iota J = \iota$. Thus $t\iota J$ is a conjugate of ι normalizing H^0, giving a contradiction as explained above. For $(H^0)' = Sp_a(q^2)$ or $G_2(q^2)$, we apply the same argument, starting with an involution τ centralizing $(H^0)'$.

To complete this case ($b = 2, q = 16$), suppose now that $(H^0)' = SL_a(q^2)$ with a odd and $a \geq 3$. Here we have

$$SL_a(q^2)\,\langle \phi, \tau \rangle < SL_{2a}(q)\,\langle \tau \rangle,$$

where $\phi \in SL_{2a}(q)$ is an involution inducing a field automorphism on $L = SL_a(q^2)$ and τ is an involutory graph automorphism of $G = SL_{2a}(q)$ normalizing L and commuting with ϕ.

We shall show that τ is G-conjugate to ι. Observe that $C_L(\phi\tau) = SU_a(q)$, hence $C_G(\phi\tau) = Sp_{2a}(q)$. Hence as above we can take $\phi\tau = \iota J$. Now $J \in C_G(\iota J)$, and $\phi \in C_G(\phi\tau) = C_G(\iota J)$. Hence $J, \phi \in C_G(\iota J) = Sp_{2a}(q)$. Both J and ϕ have Jordan form J_2^a on V, and as a is odd they are conjugate in $C_G(\iota J)$ (see Lemma 2.1); say $\phi = J^c$ with $c \in C_G(\iota J)$. Then

$$\iota^c = (\iota J J)^c = \iota J \phi = \phi\tau\phi = \tau.$$

Therefore τ is conjugate to ι, as claimed. As before this gives a contradiction. This completes the proof for the case $b = 2, q = 16$.

The remaining cases $(b, q) = (2, 8), (3, 2), (4, 2)$ are excluded in entirely the same fashion, and we leave this to the reader.

To complete the proof we justify the last sentence of the statement of the theorem, asserting the existence of antiflag transitive examples in each of conclusions (i)-(iv).

The examples in (i) are easy to justify. This is done in [7] but we give a different argument. Clearly $SL_n(q)$ is antiflag transitive. As for $Sp_n(q)$, any antiflag is of the form $(\langle v \rangle, w^\perp)$ with $w \notin v^\perp$, and $Sp_n(q)$ is transitive on such pairs (by Witt's lemma for example). Finally, for q even we have $G_2(q) < Sp_6(q)$. Since an antiflag $(\langle v \rangle, w^\perp)$ as above is stabilized by a subgroup $Sp_4(q)$ fixing $\langle v, w \rangle$ pointwise, it is enough to demonstrate the factorization $Sp_6(q) = G_2(q)\,Sp_4(q)$. Now $G_2(q)$ has a subgroup $L_2(q) \times L_2(q)$ acting on the natural 6-dimensional module V_6 as $V_4 \perp V_2$ (it acts as $\Omega_4^+(q)$ on V_4 and as $Sp_2(q)$ on V_2). Hence, if we take our subgroup $Sp_4(q)$ to fix V_2 pointwise, we have $G_2(q) \cap Sp_4(q) \cong L_2(q)$, and now arithmetic shows that $Sp_6(q) = G_2(q)\,Sp_4(q)$, as required. For completeness, we remark that when $q = 2$, while $G_2(2)$ is antiflag transitive, in fact $G_2(2)'$ is not; on the other hand $G_2(2)' \times \langle \tau \rangle$ is antiflag transitive, where τ is a suitable graph automorphism of $L_6(2)$ (all this can be seen using [9, p.14,46]).

Next we justify the examples in (ii) and (iv). First, [33, Prop. B, p.45] and its proof show that $\Gamma L_m(q^2) < \Gamma L_{2m}(q)$ is antiflag transitive for $q = 2$ or 4 (and also that the full group of field automorphisms must be present, as asserted in (ii)). Given this, the antiflag transitivity on $V_{2m}(q)$ of $\Gamma Sp_m(q^2)$ (m even) and $\Gamma G_2(q^2)$ ($m = 6$) follows from the antiflag transitivity of these groups on $V_m(q^2)$.

Finally the examples $A_6, A_7 < L_4(2) \cong A_8$ in (iii) are well known and follow immediately from the 2-transitivity (on 8 points) of the antiflag stabilizer $L_3(2)$.

■

4 Subgroups of classical groups transitive on subspaces

In this section we study subgroups of classical groups G which are transitive on a G-orbit of subspaces of the natural module for G. The basic starting point is [33], which determines all such maximal subgroups of G.

Our first lemma classifies those types of subspace which admit transitive proper subgroups of G. Recall the subgroup notations $P_i, N_i, O^\epsilon, N_{1,n-1}$ from Section 2.

Lemma 4.1 *Let G be an almost simple classical group with socle G_0, and let M be one of the following maximal subgroups of G:*

$$P_i,\ N_i,\ O^\epsilon,\ N_{1,n-1}.$$

Suppose that G contains a subgroup H which is transitive on the coset space G/M and does not contain G_0. Then one of the following holds:

(i) *$G_0 = L_n(q)$: $M = P_1, P_{n-1}$ or $N_{1,n-1}$;*

(ii) *$G_0 = U_{2m}(q)$: $M = P_m$ or N_1;*

(iii) *$G_0 = PSp_{2m}(q)$: $M = P_1, P_m, N_2$ or O^ϵ;*

(iv) *$G_0 = \Omega_{2m+1}(q)$ (q odd, $m \geq 3$): $M = P_m$, N_1^-, N_1^+ ($m = 3$) or N_2^ϵ ($m = 3$);*

(v) *$G_0 = P\Omega_{2m}^-(q)$ ($m \geq 4$): $M = P_1, N_1$ or N_2^+;*

(vi) *$G_0 = P\Omega_{2m}^+(q)$ ($m \geq 4$): $M = P_1, P_{m-1}, P_m$, N_1, N_2^ϵ or N_3 ($m = 4$);*

(vii) *exceptional cases:*

$$\begin{array}{l} G_0 = L_5(2) : M = P_2, P_3 \\ G_0 = U_3(q), q = 3, 5, 8 : M = P_1 \\ G_0 = U_4(3) : M = P_1 \\ G_0 = U_9(2) : M = P_1 \end{array}$$

Proof By hypothesis we have $G = HM$. Hence the possibilities for M are given by the tables of maximal factorizations in [33, Tables 1-4], together with Lemma 2.6. The conclusion follows. ∎

In the rest of the section we prove lemmas which give lists of possibilities for the transitive subgroups H such that $G = HM$ in the following cases:

G_0	M	reference
$PSp_{2m}(q)$	N_2, O^-	Lemmas 4.2,4.6
$U_n(q)$	N_1	Lemma 4.3
$P\Omega^{\epsilon}_{2m}(q)$	N_1	Lemmas 4.4,4.5

Note that the cases where $G_0 = L_n(q)$ and $M = P_1$ or $N_{1,n-1}$ are covered by the results of the previous section, since in these cases the factorization $G = HM$ is equivalent to saying that H is transitive on 1-spaces or antiflags, respectively.

The results in the rest of this section are less precise than those in the previous one, since we make no claim that all subgroups listed in the conclusions are actually transitive on the relevant G-orbit of subspaces. We note also that the results of Lemmas 4.4 and 4.5 cover in addition possibilities for transitive subgroups for the G-action on nondegenerate quadratic forms of type $-\varepsilon$, where $G_0 = \Omega^{\varepsilon}_{2m}(q)$ and $\varepsilon = \pm$, since this action is equivalent to the G-action on cosets of N_1.

Lemma 4.2 *Let B be a subgroup of $\Gamma Sp_{2m}(q)$ $(m \geq 2)$ not containing $Sp_{2m}(q)$, such that B is transitive on the cosets of N_2. Then one of the following holds:*

(i) $B \triangleright Sp_m(q^2)$ *(m even, $q = 2$ or 4) or $Sp_{m/2}(q^4)$ ($m/2$ even, $q = 2$);*

(ii) $B \triangleright G_2(q)'$ *($m = 3$, q even), $G_2(q^2)$ ($m = 6, q = 2$ or 4), or $G_2(q^4)$ ($m = 12, q = 2$);*

(iii) $B \triangleright SL_2(q^2)$ *($m = 2$, q even).*

Proof We have a factorization $G = BN_2$, where G is a group with $Sp_{2m}(q) \leq G \leq \Gamma Sp_{2m}(q)$. Hence by [33] together with Lemma 2.6, one of the following holds:

(α) $B \leq \Gamma Sp_m(q^2)$ ($q = 2$ or 4)

(β) $B \leq \Gamma G_2(q)$ ($m = 3$, q even)

(γ) $m = 2$.

Case (α) By [33], $N_2 \cap Sp_m(q^2) = Sp_2(q) \times Sp_{m-2}(q^2)$, which fixes an N_2-space in $V_m(q^2)$. Hence B is transitive on N_2-spaces in $V_m(q^2)$, and it follows inductively that either B is as in the conclusion, or one of:

(a) $B \trianglerighteq SL_2(q^4)$ with $m = 4$,

(b) $m = 2$.

In (a), the full normalizer of $SL_2(q^4)$ in $\Gamma Sp_8(q)$ is $SL_2(q^4).[4\log q]$, while $|G : N_2| = q^6.\frac{q^8-1}{q^2-1}$, hence q^2 divides $4\log q$, forcing $q = 2$, as in conclusion (i). In (b) we have a factorization of type $SL_2(q^2) = B\,SL_2(q)$. By [33] this forces $|B| \leq 17.8$ for $q = 4$, whereas $|G : N_2| = 4^2 \cdot 17$. And for $q = 2$ we have $G = Sp_4(2) \cong S_6$, $N_2 = S_3 \times S_3$ and $B = 5.4$; but then $B \cap N_2$ contains an involution, so $G \neq BN_2$.

Case (β) In the factorization $Sp_6(q) = G_2(q)N_2$, we have $G_2(q) \cap N_2 = L_2(q)^2$ by [33]. Hence if $B \not\geq G_2(q)'$, then there must be a factorization of type $G_2(q) = BL_2(q)^2$. There is no such factorization for $q > 2$, and for $q = 2$ we get $U_3(3).2 = B(S_3 \times S_3)$, forcing $B \leq L_2(7).2$, again by [33]. However $|B|_2 = 2^4$ and $U_3(3)$ has only one class of involutions, so $B \cap (S_3 \times S_3)$ contains an involution, showing the above factorization does not exist.

Case (γ) Here we have a factorization of type $Sp_4(q) = B\,Sp_2(q)^2$. Assume $q > 2$. By [33], q is even and $B \leq N(Sp_2(q^2))$ or $N(Sz(q))$. The latter is out, as from [33, 5.17b] we see that $Sz(q) \cap O_4^+(q) \leq \Omega_4^+(q)$, hence $Sp_4(q) \neq Sz(q)\Omega_4^+(q)$. Consequently $B \leq N(Sp_2(q^2))$. The normalizer of $Sp_2(q^2)$ in $\Gamma Sp_4(q)$ is $Sp_2(q^2).2\log q$, and $|G : N_2| = q^2(q^2+1)$. Hence either $B \trianglerighteq Sp_2(q^2)$, giving conclusion (iii), or q^2 divides $4\log q$, contrary to our assumption that $q > 2$.

Finally, if $q = 2$ then we have a factorization $S_6 = B(S_3 \times S_3)$. As above, $B = 5.4$ does not work, so we must have $B \geq A_5 = SL_2(4)$, again giving (iii).

This completes the proof of the lemma. ∎

Remark As remarked earlier, the lemma by no means asserts that all subgroups B satisfying (i) , (ii) or (iii) in the conclusion give examples which are transitive on N_2-spaces. Indeed, with a rather more delicate analysis it is possible to show that the $Sp_{m/2}(2^4)$ and $G_2(2^4)$ possibilities in (i) and (ii) do not yield transitive subgroups, but we shall not need this information.

In the next result we use the usual notation for $\Gamma U_n(q)$ as a subgroup of $\Gamma L_n(q^2)$.

Lemma 4.3 *Let B be a subgroup of $\Gamma U_n(q)$ $(n \geq 3)$ not containing $SU_n(q)$, such that B is transitive on the cosets of N_1. Then $n = 2m$ is even, and one of the following holds:*

(i) $B \triangleright Sp_{2m}(q), Sp_m(q^2)$ *(m even, $q = 2$ or 4) or $Sp_{m/2}(q^4)$ ($m/2$ even, $q = 2$);*

(ii) $B \triangleright SL_m(q^2)$ *($q = 2$ or 4) or $SL_{m/2}(q^4)$ ($m > 2$ even, $q = 2$);*

(iii) $B \triangleright G_2(q)'$ *($m = 3$, q even), $G_2(q^2)$ ($m = 6, q = 2$ or 4), or $G_2(q^4)$ ($m = 12, q = 2$);*

(iv) *one of:*

$$m = 3, q = 2 : \; B \triangleright U_4(3) \text{ or } M_{22}$$
$$m = 6, q = 2 : \; B \triangleright 3.Suz$$

(v) $B \leq P_m$, *and modulo the unipotent radical of P_m, B induces a subgroup of $\Gamma L_m(q^2)$ which is transitive on 1-spaces.*

Proof There is a factorization $G = BN_1$, where $SU_n(q) \leq G \leq \Gamma U_n(q)$. If n is odd there are no such factorizations, so n is even, say $n = 2m$. By [33] together with Lemma 2.6, one of the following holds:

(α) $B \leq P_m$

(β) $B \leq N_G(Sp_{2m}(q))$

(γ) $B \leq N_G(SL_m(q^2))$ ($q = 2$ or 4)

(δ) one of:

$$m = 3, q = 2 : \; B \leq N(U_4(3)) \text{ or } N(M_{22})$$
$$m = 6, q = 2 : \; B \leq N(3.Suz)$$

Case (α) Write $P_m = G_W$, where W is a totally isotropic m-space. From [33, p.53], we see that $N_1 \cap P_m$ fixes an $(m-1)$-subspace of W, and hence, modulo the unipotent radical of P_m we have a factorization $\Gamma L_m(q^2) = \bar{B}P_{m-1}$. Hence conclusion (v) holds.

Case (β) Assume $B \not\geq Sp_{2m}(q)$. Then from [33, p.56] we see that $N_1 \cap Sp_{2m}(q)$ is contained in an N_2-subgroup of $Sp_{2m}(q)$, and hence B is given by Lemma 4.2. All these groups are in the conclusion, apart from the case

$$B \triangleright SL_2(q^2)\ (m = 2, q \text{ even}, q > 4).$$

We rule this out. Write S for the normal subgroup $SL_2(q^2)$ of B.

First observe that $|C_{SU_4(q)}(S)|_2 = 1$: for otherwise, if t is an involution in this centralizer then $\langle t\rangle \times S$ lies in a parabolic subgroup, which must be $q^4.GL_2(q^2)$; however a Levi subgroup acts irreducibly on the unipotent radical of this parabolic, so this is not possible.

It follows that $|B|_2$ divides $|SL_2(q^2)|_2 \cdot 2\log q$, and hence as $|G : N_1|_2 = q^3$, we have $q \mid 2\log q$. This is impossible as $q > 4$.

Case (γ) By [33, p.54], $N_1 \cap SL_m(q^2)$ fixes an antiflag of the space $V_m(q^2)$. Hence B is antiflag transitive on this space, so is given by Theorem 3.2. All the possibilities for B are in the conclusion, except for

$$B = 5.4 \times 2 < SL_2(4).2 \times 2 < G = U_4(2).2.$$

We rule out this possible factorization $U_4(2).2 = BN_1$ with $B = 5.4 \times 2$. Note that if such a factorization existed then $|B \cap N_1|$ would be odd, since $|G : N_1|_2 = 8$.

Observe that $B < S_6 \times 2 = Sp_4(2) \times \langle\sigma\rangle < G$, where σ is an involutory field automorphism of $U_4(2)$ and $\sigma \in B$. We write the natural G-module $V = V_4(2^2)$ as the heart of the permutation module for S_6 - that is, as

$$V = \{(a_1, \ldots, a_6) : \sum a_i = 0\}/T,$$

where $T = \langle(1, 1, \ldots, 1)\rangle$. This space has standard $Sp_4(2)$-basis

$$\begin{aligned} e_1 &= (1, 1, 0, 0, 0, 0) + T, \quad & e_2 &= (0, 0, 1, 1, 0, 0) + T, \\ f_1 &= (1, 0, 0, 0, 0, 1) + T, \quad & f_2 &= (0, 0, 1, 0, 1, 0) + T. \end{aligned}$$

Taking this also to be a standard $U_4(2)$-basis of V, we may take σ to be the field automorphism fixing e_1, e_2, f_1, f_2.

We may take $t = (12)(34) \in B \cap S_6$. Then t sends

$$e_1 \to e_1,\ e_2 \to e_2,\ f_1 \to f_1 + e_1,\ f_2 \to f_2 + e_2.$$

Now taking ω to be an element of $\mathbb{F}_4 \backslash \mathbb{F}_2$, we check that $t\sigma$ fixes the vector $v = \omega e_1 + f_1$. This vector is nonsingular with respect to the unitary form on V, so $t\sigma \in B \cap N_1$. Thus $B \cap N_1$ has even order, and it follows that $G \neq BN_1$.

Case (δ) First suppose $m = 3, q = 2$. If $B \leq N(U_4(3))$, then since by [33] we have $N_1 \cap U_4(3).2^2 = 3^4.S_5$, we get a factorization $U_4(3).2^2 = BP_2$, and hence (again by [33]), either $B \rhd U_4(3)$ or $B \leq L_3(4).2^2$. In the latter case we get $L_3(4).2^2 = B(A_5.2)$, hence either $B \rhd L_3(4)$ or $B \leq L_3(2).2 \times 2$. Any A_5 in $L_3(4)$ is reducible, so B is transitive on 1-spaces or antiflags in $L_3(4)$, so the $L_3(2).2^2$ possibility does not occur. We conclude that in this case, $B \rhd U_4(3)$ or $L_3(4)$, as in the conclusion.

Likewise, when $B \leq N(M_{22}) = M_{22}.2$, we get a factorization $M_{22}.2 = B(L_2(11).2)$, giving either $B \rhd M_{22}$ or $B \leq L_3(4).2$. In the latter case we have $(L_2(11).2) \cap (L_3(4).2) = A_5$ and we see as above that B must contain $L_3(4)$.

Finally, consider the case where $m = 6, q = 2$ and $B \leq N(3.Suz) = 3.Suz.2$. Here we get a factorization $Suz.2 = B(3^5.L_2(11).2)$, hence either $B \geq Suz$ or $B \leq G_2(4).2$ with $G_2(4) \cap 3^5.M_{11} = 3.A_6$. In the latter case $G_2(4).2 = B(3.A_6.2)$, and this forces $B \geq G_2(4)$. This completes the proof. ■

Lemma 4.4 *Let B be a subgroup of $\Gamma O^-_{2m}(q)$ $(m \geq 2)$ not containing $\Omega^-_{2m}(q)$, such that B is transitive on an orbit of N_1-spaces. Then one of the following holds:*

(i) $B \rhd SU_m(q)$ *(m odd),* $SU_{m/2}(q^2)$ *($m/2 \geq 3$ odd, $q = 2$ or 4) or* $SU_{m/4}(q^4)$ *($m/4 \geq 3$ odd, $q = 2$);*

(ii) $B \rhd \Omega^-_m(q^2)$ *(m even, $q = 2$ or 4) or* $\Omega^-_{m/2}(q^4)$ *($m/2$ even, $q = 2$);*

(iii) *one of:*

$$\begin{aligned} &m = 2, q = 3: \ B \rhd A_5 \\ &m = 3, q = 3: \ B \rhd L_3(4) \\ &m = 3, q = 2. \end{aligned}$$

Proof Assume first that $m \geq 4$. By [33] (and Lemma 2.6), either $B \leq N(SU_m(q))$ with m odd, or $B \leq N(\Omega^-_m(q^2))$ with m even, $q = 2$ or 4. In the first case there is a factorization of type $\Gamma U_m(q) = BN_1$, which forces $B \geq SU_m(q)$, as in (i). In the second case we get $N(\Omega^-_m(q^2)) = BN_1$, and then inductively, B satisfies (i) or (ii).

It remains to handle $m < 4$. If $m = 2$ then $\Gamma O^-_{2m}(q) = \Gamma L_2(q^2)$ and $N_1 = N(SL_2(q))$. For a factorization of type $L_2(q^2) = BL_2(q)$, [33] gives

$q = 2, 3$ or 4. If $q = 2$ or 4 we have $B \triangleright \Omega_2^-(q^2)$, as in (ii). And for $q = 3$ we get $B \triangleright A_5$ as in (iii).

Finally, let $m = 3$. Here the factorization $\Gamma O_6^-(q) = BN_1$ becomes $\Gamma U_4(q) = BN(Sp_4(q))$, and hence either $B \le N(SU_3(q))$ or $B \le N(L_3(4))$ with $q = 3$. In the first case we get a factorization of type $U_3(q) = BN_1$, hence either $B \ge SU_3(q)$ or $q = 2$, as in (i) or (iii). And in the second we get $B \triangleright L_3(4)$ as in (iii) (no proper subgroups of $L_3(4)$ arise, as there is no relevant factorization of $N(L_3(4))$). ■

Lemma 4.5 *Let B be a subgroup of $\Gamma O_{2m}^+(q)$ $(m \ge 3)$ not containing $\Omega_{2m}^+(q)$, such that B is transitive on an orbit of N_1-spaces. Then one of the following holds:*

(i) *$B \triangleright X_m(q)$, $X_{m/2}(q^2)$ ($q = 2$ or 4) or $X_{m/4}(q^4)$ ($m \ge 8$, $q = 2$), where $X \in \{SL, SU, Sp\}$; moreover m is even for $X_m(q) = Sp_m(q)$ or $SU_m(q)$;*

(ii) *$B \triangleright G_2(q)'$ ($m = 6$, q even), $G_2(q^2)$ ($m = 12, q = 2$ or 4), or $G_2(q^4)$ ($m = 24, q = 2$);*

(iii) *$B \triangleright \Omega_m^+(q^2)$ (m even, $q = 2$ or 4), or $\Omega_{m/2}^+(q^4)$ ($m/2 \ge 2$ even, $q = 2$);*

(iv) *$B \triangleright SL_2(q^2)$ ($m = 4$, q even), $SL_2(q^4)$ ($m = 8$, $q = 2$ or 4), or $SL_2(q^8)$ ($m = 16$, $q = 2$);*

(v) *one of:*

$$\begin{array}{l} m = 4: \ B \triangleright \Omega_7(q) \text{ or } \Omega_8^-(q^{1/2}) \\ m = 8, q = 2 \text{ or } 4: \ B \triangleright \Omega_7(q^2) \text{ or } \Omega_8^-(q) \\ m = 16, q = 2: \ B \triangleright \Omega_7(q^4) \text{ or } \Omega_8^-(q^2) \end{array}$$

(vi) *one of:*

$$\begin{array}{l} m = 8: \ B \triangleright \Omega_9(q) \\ m = 16, q = 2 \text{ or } 4: \ B \triangleright \Omega_9(q^2) \\ m = 32, q = 2: \ B \triangleright \Omega_9(q^4) \end{array}$$

(vii) *one of:*

$$\begin{array}{l} m = 4, q = 2: \ B \triangleright A_6, A_7 \text{ or } A_9 \\ m = 4, q = 3: \ B \triangleright \Omega_8^+(2), Sp_6(2), U_4(2), A_9 \text{ or } A_6 \\ m = 6, q = 2: \ B \triangleright U_4(3) \text{ or } M_{22} \\ m = 12, q = 2: \ B \triangleright 3.Suz \text{ or } Co_1 \end{array}$$

(viii) *$B \le P_m$ or P_{m-1}, and modulo the unipotent radical, B induces a subgroup of $\Gamma L_m(q)$ which is transitive on 1-spaces.*

Proof We begin with the observation that if $B \leq P_m$ or P_{m-1}, then conclusion (viii) holds. To see this, suppose $B \leq P = \mathrm{stab}(W) = P_m$ or P_{m-1}, where W is a totally singular m-space, and take $N_1 = \mathrm{stab}(v)$. Then $v^\perp \cap W$ has dimension $m-1$, so modulo the unipotent radical of P, we have a factorization $\Gamma L_m(q) = \bar{B}P_{m-1}$. In other words $\bar{B}$ is transitive on hyperplanes of W, hence also on 1-spaces, proving (viii).

Now assume that $m = 3$. Then we have a factorization of type $SL_4(q) = BSp_4(q)$, and so by [33] and Lemma 2.6, B stabilizes either a 1-space, or a hyperplane, or an antiflag of $V_4(q)$. In the first two cases $B \leq P_i(SL_4(q))$ ($i = 1$ or 3), so $B \leq P_3(\Omega_6^+(q))$ or $P_2(\Omega_6^+(q))$, and so conclusion (viii) holds. In the third case the antiflag stabilizer $GL_3(q)$ intersects $N(Sp_4(q))$ in a subgroup of an antiflag stabilizer of $V_3(q)$, and so B is antiflag transitive on this space. Hence $B \triangleright SL_3(q)$, as in (i).

Now assume $m \geq 4$. We have a factorization $G = BN_1$ with $\Omega_{2m}^+(q) \leq G \leq \Gamma O_{2m}^+(q)$, so [33] (and Lemma 2.6) gives one of

(α) $B \leq P_m$ or P_{m-1}

(β) $B \leq N_G(SU_m(q))$ (m even)

(γ) $B \leq N_G(Sp_2(q) \otimes Sp_m(q))$ (m even, $q > 2$)

(δ) $B \leq N_G(SL_m(q))$

(ϵ) $B \leq N_G(\Omega_m^+(q^2))$ (m even, $q = 2$ or 4)

(ϕ) $B \leq N_G(\Omega_7(q))$ ($m = 4$)

(κ) $B \leq N_G(\Omega_8^-(q^{1/2}))$ ($m = 4$, q square)

(ι) $B \leq N_G(\Omega_9(q))$ ($m = 8$)

(λ) $B \leq N_G(A_9)$ ($m = 4, q = 2$)

(μ) $B \leq N_G(\Omega_8^+(2))$ or $N_G(\Omega_6^+(3))$ ($m = 4, q = 3$)

(ν) $B \leq N_G(Co_1)$ ($m = 12, q = 2$).

Case (α) In this case conclusion (viii) holds (the transitivity assertion follows from the first paragraph of this proof).

Case (β) Here $N(SU_m(q)) \cap N_1$ is contained in the stabilizer in $SU_m(q)$ of a nonsingular 1-space, giving a factorization of type $\Gamma U_m(q) = BN_1$. Hence B is given by Lemma 4.3, and all possibilities are listed in the conclusion under (i) or (ii).

Case (γ) Here $(Sp_2(q) \otimes Sp_m(q)) \cap N_1 \leq Sp_2(q) \otimes N_2(Sp_m(q))$. Hence B contains a subgroup of $\Gamma Sp_m(q)$ transitive on N_2-spaces, so is given by

Lemma 4.2. All possibilities are in the conclusion under (i), (ii) or (iv).

Case (δ) Here [33, p.63] shows that $N_G(SL_m(q)) \cap N_1$ fixes an antiflag of $V_m(q)$, hence B is antiflag transitive and is given by Theorem 3.2. The possibilities appear in (i), (ii), (vii).

Case (ϵ) Here [33, p.64] shows that $N_G(\Omega_m^+(q^2)) \cap N_1$ lies in a nonsingular 1-space stabilizer of $N_G(\Omega_m^+(q^2))$, so we have a factorization $N_G(\Omega_m^+(q^2)) = BN_1$. For $m \geq 6$, B is given inductively, and appears in the conclusion. Note that this is where the $SU_{m/2}(q^2)$ and $SU_{m/4}(q^4)$ possibilities arise in (i).

Now assume $m = 4$. We have $\Omega_4^+(q^2) \cong L_2(q^2)^2$, and N_1 of this group is a diagonal subgroup $L_2(q^2)$. Hence by [33], either $B \triangleright L_2(q^2)$ as in (iv), or B lies in a parabolic, hence is as in (viii), or $B \leq N((q^2{+}1) \times (q^2{-}1)) = N(\Omega_2^+(q^4))$. This is in (iii) for $q = 2$, and we exclude it for $q = 4$ as follows. Write $L = \Omega_8^+(4)$. By [24] we have $N = N_L(\Omega_4^+(16)) = (L_2(16)^2).2^2$, with one of the outer automorphisms interchanging the two $L_2(16)$ factors. Hence $|N_N(17 \times 15)|_2 = 2^3$. It follows that $|N_{\Gamma O_8^+(4)}(17 \times 15)|_2 \leq 2^5$. However $|G : N_1|_2 = 2^6$, so this is impossible.

Case (ϕ) In this case $N_1 \cap \Omega_7(q) = G_2(q)$, so we get a factorization $N_G(\Omega_7(q)) = BN_G(G_2(q))$. Hence by [33] one of the following holds: $B \geq \Omega_7(q)$; or B lies in a parabolic, in $N_G(\Omega_6^\epsilon(q))$, or in $N_G(\Omega_5(q))$; or $q = 3$ and $B \leq Sp_6(2)$ or S_9. In the first case we have conclusion (v); in the second and third we are back in cases (α, β, δ) (applying triality); in the fourth, applying triality we have $B \leq N(Sp_4(q) \otimes Sp_2(q))$, which is case ($\gamma$). Finally consider the last case, where $q = 3$ and $B \leq Sp_6(2)$ or S_9. By [33] we have $S_9 \cap G_2(3) = L_2(7).2$, so if $B \leq S_9$ then $S_9 = B\,(L_2(7).2)$, which forces $B \triangleright A_9$, as in (vii). Likewise, $Sp_6(2) \cap G_2(3) = 2^3.L_3(2)$, so if $B \leq Sp_6(2)$ then $Sp_6(2) = B\,(2^3.L_3(2)) \leq BP_3$; this implies that either $B = Sp_6(2)$ or $B \leq O_6^-(2)$, and in the latter case we have $O_6^-(2) = BP_2$, which forces $B \triangleright \Omega_6^-(2) \cong U_4(2)$, as in (vii).

Case (κ) Here we have a factorization $N_G(\Omega_8^-(q^{1/2})) = BN_G(G_2(q^{1/2})) \leq BN_1(O_8^-(q^{1/2}))$. Hence by Lemma 4.4, $B \triangleright \Omega_4^-(q)$ with $q = 4$ or 16, as in conclusion (iv).

Case (ι) Here we see from [33, p.144] that there is a factorization $N_G(\Omega_9(q)) = BN_1^+$, and hence $B \triangleright \Omega_9(q)$, as in (vi).

Case (λ) In this case we have $A_9 = B(L_2(8).3)$, which by [33, Theorem D] forces $B \rhd A_c$ $(5 \le c \le 9)$, as in (vii) (the A_5 and A_8 are elsewhere as $L_2(4)$ and $L_4(2)$ in (iv), (i)).

Case (μ) The $\Omega_6^+(3)$ case has been handled in (δ), so assume $B \le N_G(\Omega_8^+(2))$. Here $N_1 \cap \Omega_8^+(2) = 2^6.A_7$, so $N(\Omega_8^+(2)) = BN(2^6.A_7) \le BP_4$. If $B \not\geq \Omega_8^+(2)$, then by [33] this implies $B \le N(\Omega_7(2)), N(\Omega_6^-(2))$ or A_9. Also $|G : N_1| = 3^3 \cdot 40$ divides $|B|$. Inspection of these groups in [9] now yields $B \rhd \Omega_7(2), U_4(2), A_9$ or A_6, as in conclusion (vii).

Case (ν) Here $N_1 \cap Co_1 = Co_3$, so $Co_1 = BCo_3$. If $B \not\geq Co_1$ this gives $B \le 3.Suz.2$ or $(A_4 \times G_2(4)).2$. Also $|G : N_1| = 2^{11}(2^{12}-1)$. Hence from the factorizations of $G_2(4)$ and Suz, we see that $B \rhd G_2(4)$ or $3.Suz$, as in (ii), (vii). ■

Lemma 4.6 *Let B be a subgroup of $\Gamma Sp_{2m}(q)$ ($m \ge 2$, q even, $(m,q) \ne (2,2)$) not containing $Sp_{2m}(q)$, such that B is transitive on the coset space $Sp_{2m}(q)/O_{2m}^-(q)$. Then one of the following holds:*

(i) *$B \rhd Sp_{2a}(q^b)$ or $G_2(q^b)'$ ($ab = m$ or $3b = m$, resp.);*

(ii) *$B \rhd Sp_c(q^d)^2$ or $(G_2(q^d)')^2$ ($d \ge 1$, $cd = m$, c even; or $6d = m$, resp.);*

(iii) *$B \rhd Sp_{2c}(q^{d/2})$ or $G_2(q^{d/2})'$ ($d \ge 1$, $cd = m$ or $3d = m$, resp.);*

(iv) *$q = 2$ or 4, and B is as in* (i) - (vii) *of Lemma* 4.5*;*

(v) *one of:*

$$\begin{array}{l} m = 2, q = 4: \ B \rhd A_6 \\ m = 3, q = 4: \ B \rhd J_2 \\ m = 4, q = 2: \ B \rhd A_6 \text{ or } A_{10} \\ m = 6, q = 2: \ B \rhd J_2 \end{array}$$

(vi) *$B \le P_m$, and modulo the unipotent radical, B induces a subgroup of $\Gamma L_m(q)$ which is transitive on 1-spaces.*

Proof We have a factorization $G = BN_G(O_{2m}^-(q))$, where $Sp_{2m}(q) \le G \le \Gamma Sp_{2m}(q)$. Hence by [33] and Lemma 2.6, one of the following holds:

(α) $B \le P_m$

(β) $B \le N_G(Sp_{2a}(q^b))$ $(ab = m)$

(γ) $B \le N_G(Sp_m(q)^2)$ (m even)

(δ) $B \le N_G(\Omega_{2m}^+(q))$ ($q = 2$ or 4)

(ϵ) $B \le N_G(Sp_{2m}(q^{1/2}))$ ($q = 4$ or 16)

(ϕ) $B \le N_G(G_2(q))$ $(m = 3)$

(κ) $B \leq S_{10}$ ($m = 4, q = 2$).

Case (α) This gives conclusion (vi) (the transitivity assertion follows in the usual way, as $P_m \cap O^-_{2m}(q)$ fixes an $(m-1)$-space, by [33, p.49]).

Case (β) Here we have a factorization $N(Sp_{2a}(q^b)) = BN(O^-_{2a}(q^b))$, so B is given inductively. For $a \geq 2$ all such groups are in the conclusion. For $a = 1$ we have $N(SL_2(q^b)) = BN(q^b + 1)$ with $q^b \geq 8$ (we excluded $(m, q) = (2, 2)$ in the hypothesis). Then by [33], either B lies in a parabolic, giving (vi), or $q^b = 16$ and $B \rhd L_2(4)$, giving (iii).

Case (γ) In this case we have $O^-_{2m}(q) \cap (Sp_m(q) \wr S_2) = O^+_m(q) \times O^-_m(q)$, so we have a factorization

$$N(Sp_m(q)^2) = BN(O^+_m(q) \times O^-_m(q)).$$

In particular B must contain an element interchanging the two $Sp_m(q)$ factors.

Let $V = V_{2m}(q)$, and let $V = W_1 \perp W_2$ be the decomposition preserved by $Sp_m(q) \wr S_2$, where W_1, W_2 are non-degenerate m-spaces. Write $H = N_G(Sp_m(q)^2)$, $A = N_G(O^-_{2m}(q))$, and let B_0 be the subgroup of index 2 in B fixing W_1 and W_2. Then as $H \cap A$ fixes W_1, W_2, we have

$$H^{W_i}_{W_i} = B^{W_i}_0 (H \cap A)^{W_i} \quad (i = 1, 2),$$

giving factorizations of type

$$Sp_m(q) = B^{W_1}_0 O^+_m(q) = B^{W_2}_0 O^-_m(q).$$

As $B^{W_1}_0 \cong B^{W_2}_0$, it follows using [33] that $B^{W_i}_0 \leq N(Sp_c(q^d))$ or $N(G_2(q^d))$ with $cd = m$ or $6d = m$ respectively, giving further factorizations of type $Sp_c(q^d) = B^{W_1}_0 O^+_c(q^d) = B^{W_2}_0 O^-_c(q^d)$ or $G_2(q^d) = B^{W_1}_0 (SL_3(q^d).2) = B^{W_2}_0 (SU_3(q^d).2)$. From this and [33], taking d maximal, we conclude that

$$B^{W_1}_0 \cong B^{W_2}_0 \rhd Sp_c(q^d) \text{ or } G_2(q^d)' \ (cd = m \text{ or } 6d = m).$$

Thus $B \rhd Sp_c(q^d)^a$ or $G_2(q^d)^a$ with $a = 1$ or 2, as in (ii) or (iii).

Case (δ) Here $O^-_{2m}(q) \cap O^+_{2m}(q) \leq N_1(O^+_{2m}(q))$, so we have a factorization $N(O^+_{2m}(q)) = BN_1$. Thus B is given by Lemma 4.5 (with $q = 2$ or 4), as in (iv) or (vi).

Case (ϵ) In this case $O^-_{2m}(q) \cap Sp_{2m}(q^{1/2})$ normalizes $O_{2m-1}(q^{1/2})$, so we have a factorization $N(Sp_{2m}(q^{1/2})) = BP_1$. Thus B is given by Lemma 3.1.

We cannot have $B \leq \Gamma L_1(q^m)$, as $\Gamma L_1(q^m) \cap N(Sp_{2m}(q^{1/2})$ does not have order divisible by $|Sp_{2m}(q) : O^-_{2m}(q)| = q^m(q^m-1)/2$. Also the case where $m = 2, q = 4$, $B \triangleright A_7$ is out, as $A_7 \not\leq Sp_4(2)$. The remaining possibilities for B are in the conclusion.

Case (ϕ) Here $O^-_6(q) \cap G_2(q) = SU_3(q).2$, so we have $N(G_2(q)) = BN(SU_3(q))$. If $B \not\geq G_2(q)$, it follows that $q = 4$ and $B \leq J_2.2$ or $G_2(2) \times 2$. In the first case we get a factorization $J_2.2 = B(5^2.(4 \times S_3)$, which implies either $B \triangleright J_2$ as in (v), or $B \leq G_2(2)$. Finally, if $B \leq G_2(2) \times 2$ then the fact that $|B|$ is divisible by $2^7 \cdot 63$ forces $B \triangleright U_3(3) = G_2(2)'$, as in (iii).

Case (κ) Here $N_1 \cap S_{10} = S_7 \times S_3$. Hence $S_{10} = B(S_7 \times S_3)$, so B is 3-homogeneous of degree 10, whence $B \triangleright A_6$ or A_{10}, as in (v). ■

5 Proof of Theorem 1.1: linear groups

In this section we prove Theorem 1.1 in the case where the simple group L is a linear group $L_n(q)$ which is not isomorphic to an alternating group (so we assume $(n, q) \neq (2, 4), (2, 5), (4, 2)$). Write $Z = Z(SL_n(q))$.

Suppose then that G has socle $L = L_n(q)$, acts primitively on a set Ω, and possesses a subgroup B which acts regularly on Ω. Let $\alpha \in \Omega$ and write $A = G_\alpha$, so that we have

$$G = AB,\ A \cap B = 1,\ \text{ and } A \text{ max } G.$$

By [33] together with Lemma 2.6, one of the following holds:

(5.1) $n \geq 3$ and $A = P_1, P_{n-1}$ or $N_{1,n-1}$;

(5.2) $A \triangleright PSp_n(q)$ (n even, $n \geq 4$) and $B \leq P_1, P_{n-1}$ or $N_{1,n-1}$;

(5.3) $A \triangleright SL_a(q^b)/Z$ ($ab = n$, $a \geq 2$, b prime), and either $B \leq P_1$, P_{n-1}, or $b = 2$, $q \in \{2, 4\}$ and $B \leq N_{1,n-1}$;

(5.4) $A \leq \Gamma L_1(q^n)/Z_{q-1}$ (n odd prime) and $B \leq P_1$, P_{n-1};

(5.5) $L = L_2(q)$, $L_3(4)$ or $L_5(2)$.

Case (5.1) If $A = P_1$ or P_{n-1} then $|B| = |G : A| = \frac{q^n-1}{q-1}$, and B is transitive on the set of 1-spaces in $V = V_n(q)$. Hence by Lemma 3.1 we have $B \leq \Gamma L_1(q^n)/\mathbb{F}_q^*$, as in line 1 of Table 16.1. A complete description of the regular subgroups in this case can be deduced from [14].

If $A = N_{1,n-1}$ then $|B| = |G : A| = q^{n-1}.\frac{q^n-1}{q-1}$ and B is antiflag transitive on V, hence is given by Theorem 3.2. By arithmetic the only possibility occurs when $n = 4, q = 2$, but this was excluded by assumption (because $L_4(2) \cong A_8$).

Case (5.2) Here

$$|B| = |G : A| = \frac{1}{d} q^{(n^2-2n)/4}(q^{n-1} - 1)(q^{n-3} - 1) \dots (q^3 - 1),$$

where d divides $(n, q-1)$ (see [25, 4.8.3]).

Suppose first that $B \le P_1$. Since $G = AB$ we have $P_1 = B(A \cap P_1)$. Write $P_1 = QR$ where $Q = (\mathbb{F}_q)^{n-1}$ is the unipotent radical and $R \triangleright SL_{n-1}(q)$ a Levi subgroup. Working modulo Q, and writing $\bar{B} = BQ/Q$, we obtain a factorization $N(SL_{n-1}(q)) = \bar{B}\, N(Sp_{n-2}(q))$. In particular $\bar{B}$ is transitive on 1-spaces in $V_{n-1}(q)$, and so by Lemma 3.1 (noting that $n-1$ is odd) we have either $\bar{B} \triangleright SL_c(q^d)$ $(cd = n-1, c \ge 3)$ or $\bar{B} \le \Gamma L_1(q^{n-1})$. Since $|B| = |G : A|$ is divisible by $q^{n-3} - 1$, this is clearly impossible unless $n = 4$. In this case $B \le Q.\Gamma L_1(q^3)$ with $|Q| = q^3$ and $|B| = \frac{1}{d} q^2(q^3 - 1)$. As q^2 does not divide $3 \log q$ this forces $B \cap Q \ne 1$. However this is impossible, as $\bar{B}$ acts irreducibly on Q. The same argument deals with $B \le P_{n-1}$.

A very similar argument applies when $B \le N_{1,n-1}$: the factorization $N_{1,n-1} = B(A \cap N_{1,n-1})$ gives $N(SL_{n-1}(q)) = B\, N(Sp_{n-2}(q))$, which leads to a contradiction using the above argument.

Case (5.3) Suppose first that $B \le P_1 = QR$ as above (the argument below also deals with the case where $B \le P_{n-1}$). Now $A \cap P_1$ fixes an $\mathbb{F}_{q^b}$ 1-space containing the $\mathbb{F}_q$ 1-space fixed by P_1. Hence, working modulo Q with the factorization $P_1 = B(A \cap P_1)$ yields a factorization

$$N(SL_{n-1}(q)) = \bar{B} P_{b-1}$$

where $\bar{B} = BQ/Q$ and P_{b-1} is the stabilizer of a $(b-1)$-space in $V_{n-1}(q)$. By [33] this implies that either $b = 2$ or $L = L_6(2)$, $b = 3$ and $|\bar{B}| = 31 \cdot 5$. In the latter case $|B|$ divides $2^6 \cdot 31 \cdot 5$, which is less than $|G : A|$, a contradiction.

Hence $b = 2$ and $n = 2a$ is even. Moreover, Lemma 3.1 implies that $\bar{B} \le \Gamma L_c(q^d)$ with $cd = n - 1$. As $|G : A|$ is divisible by $q^{n-3} - 1$ this forces $n = 4$ and $B \le Q.\Gamma L_1(q^3)$. Here

$$|B| = |G : A| = \frac{1}{2} q^4 (q^3 - 1)(q - 1).$$

Hence q must divide $6 \log q$, forcing $q = 2, 3$ or 4. The first case is out as we are assuming $L \ne L_4(2)$. In the second and third cases we get the possibilities

(a) $q = 3 : G = L_4(3).2 = PGL_4(3),\ A = (4 \times L_2(9)).2^2,\ B = 3^3.13.3.2$

(b) $q = 4 : G = L_4(4).2$ (field aut.), $A = (5 \times L_2(16)).4,\ B = 2^6.\Gamma L_1(2^6)$.

Each of these gives examples in Table 16.1. To see this in case (a), note first that the elements of order 3 in A have Jordan form J_2^2, whereas those in B do not; hence $|A \cap B|_{2'} = 1$. Furthermore $A \geq P\Gamma L_2(9)$, $A \cap L \geq P\Sigma L_2(9)$, and $P\Gamma L_2(9) \backslash P\Sigma L_2(9)$ contains no involution, whereas B does. Hence $A \cap B = 1$, and we have an exact factorization $G = AB$.

The argument for (b) is quite similar. Since the normal 2^6 in B consists of transvections (and the identity), it intersects A trivially. The elements of B of order dividing 3 form an elementary abelian subgroup, generated by the matrix diag$(1, \omega, \omega, \omega)$ and a field automorphism acting on the ω-eigenspace viewed as $\mathbb{F}_{64}$ (where $\omega^3 = 1$). Hence the elements of order 3 in B have 1 as an eigenvalue, whereas those in A do not. Therefore $A \cap B \cap L = 1$. Finally, $A \cap B$ cannot contain an involution since there are no involutions in $L_2(16).4 \backslash L_2(16).2$. Consequently $A \cap B = 1$ and we have an exact factorization $G = AB$.

Now suppose that $B \leq N_{1,n-1}$ with $b = 2$ and $q = 2$ or 4. Then $A \cap N_{1,n-1}$ fixes an antiflag in $V_{n-1}(q)$ (see [33, p.46]), and so B is antiflag transitive on this space. As $n-1$ is odd, by Theorem 3.2 this forces $B \geq SL_{n-1}(q)$. But then it is impossible that $|B| = |G : A|$.

Case (5.4) Here $A \leq \Gamma L_1(q^n)/Z_{q-1}$ with n an odd prime, and we can take $B \leq P_1$. Write $P_1 = QR$ as above. Observe that $|A \cap P_1|$ divides $n \log q$.

Assume first that B contains the subgroup QS of P_1, where $S = SL_{n-1}(q)$. For the moment identify $V = V_n(q)$ with the field $F = \mathbb{F}_{q^n}$. Taking $A \leq \Gamma L_1(F)$, it is then the case that A contains the Frobenius map ϕ of order n sending $x \to x^q$ for all $x \in F$. As an element of $GL_n(q)$, ϕ has determinant 1 and fixes the vector $1 \in F$. Hence ϕ lies in the subgroup QS, and it follows that $\phi \in A \cap B$, which is a contradiction.

Hence B does not contain QS. Since $P_1 = B(A \cap P_1)$, it follows that $S = SL_{n-1}(q)$ has a proper subgroup of index dividing $n \log q$. Using [25, 5.2.2], we see that this forces $n = 3$ and $q = 2, 3, 4$ or 9, giving the possibilities

G	A	B
$L_3(2)$	7.3	D_8
$L_3(3)$	13.3	$3^2.[16]$
$L_3(4).S_3$	$7.3 \times S_3$	$2^4.(3 \times D_{10}).2$
$L_3(9).2$	$91.3.2$	$3^4.(8 \circ 2A_5).2^2$

The first two lines are examples; the first is recorded as $L_2(7) = P_1 D_8$ in

Table 16.1, and in the second, the normal 3^2 is the unipotent radical of a parabolic $P_1 = 3^2.GL_2(3)$, the subgroup [16] being a Sylow 2-subgroup of $GL_2(3)$. The fourth line is not an example, as $2A_5 < SL_2(9)$ is not normalized by an involutory field automorphism. The third line does give an example in Table 16.1. To see this, take $G = P\Gamma L_3(4) = L.3.2_2$ (notation of [9, p.23]). There is a factorization $PGL_3(4) = (7.3\times 3)P_1$ with $P_1 = 2^4.(3\times A_5)$, and the two factors intersect in a group of order 3 (not centralizing A_5 in P_1). Hence we see that $(7.3\times 3)\cap 2^4.(3\times D_{10}) = 1$. Moreover, the quotient $B/2^4 = (3\times D_{10}).2$ is of index 2 in $S_3 \times F_{20}$ (where F_{20} is a Frobenius group of order 20), and contains no involution lying outside $3 \times D_{10}$. Consequently $A \cap B = 1$ and we have an exact factorization $G = AB$.

Case (5.5) If $L = L_5(2)$, then the maximal factorization not yet considered has factors 31.5 and P_2 (or P_3). This gives the exact factorizations in Table 16.1, with A and B either factor:

$$L_5(2) = P_i\ (31.5) = (31.5)\ P_i\ \ (i = 2, 3)$$

If $L = L_3(4)$, the maximal factorization not yet considered is

$$L_3(4).2_1 = (L_3(2).2)\ (A_6.2).$$

The intersection of the factors has order 6. Now the factor $A_6.2$ is M_{10}, so has no subgroup of index 6. On the other hand, the index of M_{10} in G is 56, and $L_3(2).2$ has no subgroup of order 56. Hence no exact factorizations arise in this case.

It remains to deal with $L = L_2(q)$, $q > 5$. The maximal factorizations of groups with socle L are given by [33], and in particular one of the following holds:

(α) $A = P_1$

(β) $A \cap L = D_{2(q+1)/(2,q-1)}$, $B \leq P_1$

(γ) $A \cap L = A_5, S_4$ or A_4.

Consider (α), where $A = P_1$. Here B has order $q+1$. We can assume B is not as in line 1 of Table 16.1, so $B\cap L \leq A_5, S_4$ or A_4. If $B\cap L \leq A_5$, then q is one of $59, 29, 19, 11$. For $q = 59$, we get the exact factorization $L_2(59) = P_1\ A_5$, as in Table 16.1. For $q = 29$, there is no suitable subgroup B. If $q = 19$, the only possibility is the exact factorization $PGL_2(19) = P_1\ (5.4)$ – but this is as in line 1 of Table 16.1. And if $q = 11$, we get the exact factorization $L_2(11) = P_1\ A_4$ in Table 16.1.

If $B \cap L \leq S_4$ then q is either 7 or 23, and we get the exact factorization $L_2(23) = P_1\ S_4$ (the only $q = 7$ examples are in line 1 of Table 16.1). Finally, if $B \cap L \leq A_4$ then $q = 11$, leading again to the example $L_2(11) = P_1\ A_4$.

Next consider (β): $A \cap L = D_{2(q+1)/(2,q-1)}$, $B \leq P_1$. Note that $|G : A| = q(q-1)/2 = |B|$. If $q \equiv 3 \bmod 4$ then $A \cap P_1 \cap L = 1$ and we have exact factorizations as in Table 16.1. Note that if $q = 7$, then A only becomes maximal in $PGL_2(7)$. If $q \not\equiv 3 \bmod 4$, for an exact factorization, no involution of $PGL_2(q)$ can be contained in B. Hence the Sylow 2-subgroup of B, of order equal to the 2-part of $q(q-1)/2$, would have to consist of field automorphisms. An easy calculation shows this is only possible for $q = 4$, a case excluded here.

Finally consider case (γ). If $A = A_5$ then either $G = L$ with q one of $59, 29, 19, 11$ and $B \leq P_1$, or $G = L_2(16).4$. The former leads to the examples $L_2(59) = A_5\ (59.29)$, $L_2(29) = A_5\ (29.7)$, and $L_2(11) = A_5\ 11$. There is no regular subgroup in the cases $q = 19$ and $q = 16$, since the elements of order 3, respectively 2 in L are not fixed point free. This argument also disposes of the possibility that $q = 16$ and $A \cap L = D_{34}$, since the degree is 120.

If $A \cap L = S_4$ then q is 7 or 23. The former leads to the example $L_3(2) = P_1\ 7$ in line 1 of Table 16.1, while the latter gives the exact factorization $L_2(23) = S_4\ (23.11)$ in the table.

Finally, if $A \cap L = A_4$, then $q = 11$ and $G = PGL_2(11)$. We get the example $PGL_2(11) = S_4\ (11.5)$, which is recorded in the table with the sign † indicating that outer automorphisms are needed in G for maximality of A in G (see the beginning of Section 16).

6 Proof of Theorem 1.1: unitary groups

In this section we prove Theorem 1.1 in the case where the simple group L is a unitary group $U_n(q)$ with $n \geq 3$ and $(n, q) \neq (3, 2)$. Suppose then that G has socle $L = U_n(q)$, acts primitively on a set Ω, and possesses a subgroup B which acts regularly on Ω. Let $\alpha \in \Omega$ and write $A = G_\alpha$, so that $G = AB$, $A \cap B = 1$ and A max G. By [33] and Lemma 2.6, one of the following holds:

(6.1) n is even and $A = N_1$;

(6.2) n is even and $B \leq N_1$;

(6.3) $L = U_3(3), U_3(5), U_3(8), U_4(2), U_4(3)$ or $U_9(2)$.

Case (6.1) In this case we have, writing $n = 2m$,

$$|B| = |G : N_1| = q^{2m-1}.\frac{q^{2m}-1}{q+1}. \tag{2}$$

Moreover, B satisfies the conclusion of Lemma 4.3. None of the possibilities given in (i), (ii), (iii) or (iv) of the lemma can satisfy (2). So suppose $B \le P_m$, as in (v) of Lemma 4.3. Write $P_m = QR$, with Q the unipotent radical and $R \triangleright SL_m(q^2)$, so that $\bar{B} = BQ/Q$ is transitive on the 1-spaces in $V_m(q^2)$. Then by Lemma 3.1, one of the following holds:

(a) $\bar{B} \triangleright SL_a(q^{2b})$ $(ab = m, a \ge 2)$, $Sp_a(q^{2b})$ $(ab = m,\ a$ even$)$ or $G_2(q^{2b})$ $(6b = m,\ q$ even$)$

(b) $m = 2, q = 3$ and $\bar{B} \triangleright A_5$

(c) $\bar{B} \le GL_1(q^{2m})$.

Case (a) is not possible by (2). And case (b) is out, as there is no subgroup $3^2.A_5$ in $P_2 = 3^4.L_2(9)$.

Now consider case (c), $\bar{B} \le GL_1(q^{2m})$. Assume for the time being that $(q, 2m) \ne (2, 6)$, and let $t \in B$ be an element of order q_{2m} (see Section 2 for notation). Now $|Q| = q^{m^2}$, and as an $SL_m(q^2)$-module over $\mathbb{F}_q$, we have $Q \cong V \otimes V^{(q)}$ realised over $\mathbb{F}_q$, where $V = V_m(q^2)$. Obviously any t-invariant subgroup of Q on which t acts nontrivially has order at least q^{2m}, and hence by (2), we have $B \cap Q \le C_Q(t)$.

If λ denotes a primitive q_{2m}th root of unity in the algebraic closure $\bar{\mathbb{F}}_q$, then since it is fixed by the Frobenius q^2-power map, t acts on $V \otimes \bar{\mathbb{F}}_q$ as $\mathrm{diag}(\lambda, \lambda^{q^2}, \ldots, \lambda^{q^{2m-2}})$. As $Q \cong V \otimes V^{(q)}$, it follows that $|C_Q(t)|$ is 1 if m is even, and is q^m if m is odd.

If m is even, then $B \cap Q = 1$, so it follows from (2) that q^{2m-1} divides $2m \log q$. This is impossible as $m \ge 2$. Likewise, if m is odd then $|B \cap Q| \le q^m$, so q^{m-1} divides $2m \log q$, which is impossible as $m \ge 3$.

It remains to handle the excluded case $(q, 2m) = (2, 6)$. In this case let $t \in B$ be an element of order 7. As above we calculate that $C_Q(t) = 1$, and the composition factors of $Q \downarrow \langle t \rangle$ have order 2^3. As $|B| = 2^5 \cdot 21$, this forces 2^2 to divide $2m \log q = 6$, a contradiction.

Case (6.2) Again write $n = 2m$. In this case $B \le N_1$ and by [33], one of the following holds:

(a) $A = P_m$;

(b) $A \triangleright PSp_{2m}(q)$ or $SL_m(q^2)$ $(q = 2$ or $4)$;

(c) $L = U_6(2)$, $A \triangleright U_4(3)$ or M_{22}; or $L = U_{12}(2)$, $A \triangleright Suz$.

We have a factorization $N_1 = B(A \cap N_1)$, and $N_1 \triangleright SU_{2m-1}(q)$. Since $|B| = |G : A|$, we have $B \not\geq SU_{2m-1}(q)$ by arithmetic. Hence it follows from the factorizations of unitary groups of odd dimension in [33] that

$$L = U_4(q)\ (q = 2, 3, 5, 8) \text{ or } U_{10}(2).$$

The last case $L = U_{10}(2)$ is not possible, as it requires $A \cap N_1 \leq N(J_3)$ (see [33, Table 3]), whereas from the proofs of the factorizations $G = AN_1$ in [33] it is clear that this cannot be the case.

Now consider $L = U_4(2)$. If $A = P_2$ then $|B| = |G : A| = 27$, and there are examples of such regular subgroups in $N_1 = GU_3(2)$, as recorded in Table 16.1: for example, relative to an orthonormal basis of $V = V_4(2^2)$, define

$$a = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \omega & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega^2 \end{pmatrix}, \quad b = \mathrm{diag}(1, \omega, \omega^2, 1),$$

where $\omega^3 = 1$. Then $a^3 = (\omega I_3, 1)$ and $a^b = a^4$, so $\langle a, b\rangle = 9.3$. Elements of order 3 in A are conjugate to $(\omega, \omega, \omega^2, \omega^2)$, whereas elements of order 3 in $\langle a, b\rangle$ are in $\langle a^3, b\rangle$. Hence $\langle a, b\rangle$ is regular on $(L : A)$.

Now suppose $A \triangleright Sp_4(2)$ (still with $L = U_4(2)$). Then $|B| = 36$; however we see from [9] that A contains representatives of all classes of involutions in $U_4(2).2$, so there is no regular subgroup B in this case.

Next let $L = U_4(3)$. The only proper factorization of $U_3(3)$ is $L_2(7)P_1$. Hence $A = P_2$, $|B| = |G : A| = 112$, and from [9, p.52] we see that $B \leq (L_2(7) \times 4).2$. But this group has no subgroup of order 112.

Now consider $L = U_4(5)$. The only factorization of $U_3(5)$ is A_7P_1, so $A = P_2$, $|B| = 756$ and $B \leq 2 \times 3.S_7$. However $2 \times 3.S_7$ has no subgroup of order 756.

Finally, let $L = U_4(8)$. Again $A = P_2$ so $|B| = 3^5 \cdot 19$, and $B \leq N_1$. In order to have a subgroup B of this order in $N_1 = N_1(G)$ we require $G = L.3$ and the only possibility for B is $GU_1(29).9 < N_1 = GU_3(8).3$. This is an example in Table 16.1: arguing as in the case above where $L = U_4(2), A = P_2$, we see that no element of order 3 in $B \cap L = (29 + 1).3$ is conjugate to an element of order 3 of P_2; hence $A \cap B \cap L = 1$. Finally $B \backslash ((B \cap L)$ has no element of order 3, hence also $A \cap B = 1$, so we have an exact factorization $G = AB$.

Case (6.3) There are six possible socles to consider here:

$$L = U_3(3), U_3(5), U_3(8), U_4(2), U_4(3) \text{ or } U_9(2).$$

We consider possible maximal factorizations of G containing our factorization AB.

Let $L = U_3(3)$. The maximal factorization of L to consider has factors P_1 and $L_2(7)$, intersecting in a subgroup of order 6. An inspection of the permutation characters of $G = U_3(3).2$ of degrees 28 and 36 shows that there are no fixed-point-free involutions in either action.

Let $L = U_3(5)$. The maximal factorization of L to consider has factors P_1 and A_7, intersecting in a subgroup of order 20. If $A = P_1$ then A_7 must have a proper subgroup of order divisible by 63 - not so. Hence A normalizes A_7 and B is regular of order 50. This is not possible, since an inspection of the permutation character shows that all involutions fix points in this action.

Let $L = U_3(8)$. Here the maximal factorization to consider is in fact exact:

$$U_3(8).3^2 = P_1\ (3 \times 19.9) = (3 \times 19.9)\ P_1$$

as in Table 16.1.

Let $L = U_4(2)$. Here the maximal factorization of L not already considered (in (6.1), (6.2)) has factors $3^3.S_4$ and P_2, of index 40 and 27. From the permutation character of degree 40 we see that all involutions in G fix a point in this action. Hence $A = P_2$, of index 27. We have seen an exact factorization

$$U_4(2) = P_2\ [27]$$

in the above case (6.2). The Magma computations of Michael Giudici (mentioned in the remarks after Theorem 1.1) show that up to L-conjugacy there are two regular examples $B = [27]$, which are in fact non-isomorphic.

Let $L = U_4(3)$. Here one of the factors of a maximal factorization containing AB intersects L in $L_3(4)$, the other in one of P_1, P_2 and $PSp_4(3)$. Assume A normalizes $L_3(4)$, so B has order 162. Since L has a unique class of involutions, G must contain some outer involutory automorphisms. We claim that there is an exact factorization

$$U_4(3).2 = (L_3(4).2)\ (3^4.2).$$

This follows from the argument in [33, p. 113]: let $G = U_4(3).2_1$ in the notation of [9, p. 52], and $A = N_G(L_3(4)) = L_3(4).2_2$. Now $G = AP_2$, and $P_2 = 3^4.(2 \times A_6)$, with $A \cap P_2 = A_6$. It is then clear that the normal subgroup $B = 3^4.2$ of P_2 is an example of a regular subgroup of degree 162. In fact there are more examples — the computations of Giudici show that there are 6 classes of regular subgroups B of order 162 in $G = U_4(3).2^2$, all pairwise non-isomorphic.

If A is one of the other factors (namely P_1, P_2 or $PSp_4(3)$), then the degree $|G : A|$ is $280, 112$ or 126, and B is a subgroup of $N_G(L_3(4))$ of this order. However, $L_3(4).2^2$ has no subgroups of any of these orders, since the only maximal subgroup of $L_3(4)$ of order divisible by 7 is $L_2(7)$.

Finally let $L = U_9(2)$. The relevant maximal factorization of L has factors P_1 and J_3, with intersection $2^{2+4}.(3 \times S_3)$. Since J_3 has no proper factorizations, A must be $N_G(J_3)$ and L has index at most 2 in G. Now the derived subgroup of the Levi subgroup of P_1 is $U_7(2)$; since this has no proper factorizations, it must be involved in B. Considering the power of 3, this is impossible as B is regular.

7 Proof of Theorem 1.1: orthogonal groups in odd dimension

In this section we prove Theorem 1.1 in the case where G has socle $L = \Omega_{2m+1}(q)$ ($m \geq 3$, $q = p^a$ odd).

Suppose $G = AB$, $A \cap B = 1$ and A max G. By [33] and Lemma 2.6, one of the following holds:

(7.1) $A = N_1^-$;

(7.2) $A = P_m$, $B \leq N_1^-$;

(7.3) $m = 3$ and either $A = N_G(G_2(q))$ or $B \leq N_G(G_2(q))$;

(7.4) $q = 3^e$, $L = \Omega_{13}(q)$ or $\Omega_{25}(q)$ and $A = N(PSp_6(q))$ or $N(F_4(q))$, respectively;

(7.5) $L = \Omega_7(3)$.

Case (7.1) Here $|B| = |G : N_1^-| = \frac{1}{2}q^m(q^m - 1)$. For any involution $t \in SO_{2m+1}(q)$, either the 1-eigenspace or the -1-eigenspace of t is a non-degenerate subspace of dimension at least 4, and hence t lies in a conjugate of N_1^-. In other words $A = N_1^-$ contains representatives of all involution classes of $G \cap SO_{2m+1}(q)$, and hence $B \cap SO_{2m+1}(q)$ has odd order. It follows that $|B|_2$ divides $\log_p q$. This is only possible if $|B|$ is odd - in other words, m is odd and $q \equiv 3 \bmod 4$.

By [33], the factorization $G = BN_1^-$ implies that either $B \leq P_m$ or $B \leq N(G_2(q))\,(m = 3)$. In the latter case we get an exact factorization

$N(G_2(q)) = B\,(N_1^- \cap N(G_2(q))$. However there is no such exact factorization by [33, Theorem B].

Hence $B \leq P_m$. Write $P_m = QR$, where Q is the unipotent radical and the Levi subgroup $R \triangleright SL_m(q)$. Working modulo Q with the factorization $P_m = B(A \cap P_m)$, we get a factorization of type $SL_m(q) = \bar{B}P_{m-1}$, where $\bar{B} = BQ/Q$. As $|B|$ is odd, it follows by Lemma 3.1 that $\bar{B} \leq \Gamma L_1(q^m)$.

Relative to a standard basis $e_1, \ldots, e_m, d, f_1 \ldots, f_m$ of $V = V_{2m+1}(q)$ (see [25, 2.5.3]), Q consists of matrices of the form

$$\begin{pmatrix} I_m & 0 & 0 \\ x & 1 & 0 \\ Y & -x^T & I_m \end{pmatrix},$$

where x is $1 \times m$, Y is $m \times m$, and $Y + Y^T = -x^T x$. Denote such a matrix by $M(x, Y)$. The conjugation action of an element g in the Levi subgroup $GL_m(q)$ sends $M(x, Y) \to M(xg, g^T Y g)$.

We have $Q' = Z(Q) = \{M(0, Y) \,:\, Y + Y^T = 0\}$. Moreover, Q' and Q/Q' are irreducible $\mathbb{F}_q SL_m(q)$-modules, isomorphic to $\wedge^2 V^*$ and V respectively, where $V = V_m(q)$.

Let $t \in B$ be an element of prime order $q_m = p_{me}$, where $q = p^e$, and let $Q_0 = B \cap Q$. Now $C_Q(t) = 1$, and hence every composition factor of $Q \downarrow \langle t \rangle$ has order q^m. Since Q_0 is t-invariant, and $|B| = \frac{1}{2}q^m(q^m - 1)$, it follows that Q_0 has order q^m. Also Q_0 is abelian (as $Z(Q_0)$ is t-invariant). Moreover $Q_0 \leq Q'$, since otherwise the irreducibility of $\langle t \rangle$ on Q/Q' would imply that $Q = Q_0 Q' = Q_0 Z(Q)$, which is a contradiction as Q is non-abelian.

Let $u = M(0, Y) \in Q_0$. Under the action of the Levi $GL_m(q)$, u is conjugate to $M(0, Z)$, where

$$Z = \begin{pmatrix} 0 & 0 & I_r \\ 0 & 0_{m-2r} & 0 \\ -I_r & 0 & 0 \end{pmatrix}$$

for some r. Then u has Jordan form $(J_2^{2r}, J_1^{2m-4r+1})$. As m is odd, we have $2m - 4r + 1 \geq 3$. But then Lemma 2.4(iii) implies that a conjugate of u lies in $A = N_1^-$, contradicting the exactness of the factorization $G = AB$.

Case (7.2) Here $|B| = |G : A| = \prod_{i=1}^m (q^i + 1)$, and writing $N_1^- = G_{\langle v \rangle}$, we see from [33, p.57] that $A \cap N_1^-$ fixes a totally isotropic $(m-1)$-space in $v^\perp$. Hence the factorization $N_1^- = B(A \cap N_1^-)$ gives $N(\Omega_{2m}^-(q)) = BP_{m-1}$. By [33] there is no such factorization, except for $m = 3$, in which case this becomes $N(U_4(q)) = BP_1$, which yields $q = 3$ and $B \le N(L_3(4))$. However the fact that 5 and 7 divide $|B|$ then implies that $B \ge L_3(4)$ (see [9, p.23]), which is clearly not the case.

Case (7.3) Suppose first that $A = N(G_2(q))$. By [33, Lemma A, p.105], if we embed $L = \Omega_7(q)$ irreducibly in $H = P\Omega_8^+(q)$ via a spin representation, then we have $H = LN_1$ and $L \cap N_1 = G_2(q)$. Hence the action of G on G/A is contained in that of H on H/N_1. In Section 9 we prove that the latter action has no regular subgroups for q odd (see the proof of Lemma 9.4).

Now suppose that $B \le N_G(G_2(q))$. Then we have an exact factorization $N_G(G_2(q)) = B\,(A \cap N_G(G_2(q)))$. However, $G_2(q)$ and its automorphism groups have no exact factorizations, by [33, Theorem B]. Hence there are no regular subgroups in this case.

Case (7.4) Here $B \le N_1^-$ and we have a factorization $N_1^- = B(A \cap N_1^-)$. But it is easy to see using [33] that there is no such factorization with $|B| = |G : A|$.

Case (7.5) Here $L = \Omega_7(3)$. The relevant maximal factorizations are discussed in detail in [33, pp. 100-103].

If $A = N_1^+$ then the degree $|G : A|$ is $378 = 2.3^3.7$, and relevant maximal factorizations of L have the other factor either $Sp_6(2)$ or S_9. In the first of these, the interesection of the factors is a subgroup of a parabolic subgroup P_1 of $Sp_6(2)$. This gives rise to a factorization of $Sp_6(2)$, so B must be contained in $G_2(2)$ or $L_2(8).3$; however, there is no subgroup of the right order. In the second case, S_9 has no subgroup of order 378: this would have to be transitive, containing a 7-cycle and hence 3-transitive, not so.

The case where $A = G_2(3)$ has been handled in (7.3) already.

If $A = P_3$, the degree is $1120 = 2^5.5.7$ and the relevant maximal factorizations of L have the other factor one of $S_9, Sp_6(2)$ and $2^6.A_7$. Now S_9 has no subgroup of order 1120: a subgroup of order divisible by both 7 and 5 has to involve A_7. The same is true for $Sp_6(2)$: the only maximal subgroup of order divisible by 35 is S_8, and the above applies. And the same is true also for the remaining possibility, $2^6.A_7$.

If $A = Sp_6(2)$, the degree is $3^5 13$ and the relevant maximal factorizations of G have the other factor one of $G_2(3), N_1^+$ and P_3. Now $G_2(3)$ has no exact factorizations, so the first possibility is out. In the second case, B must be contained in the parabolic $3^3 L_3(3)$ of $L_4(3)$; that however has no subgroup of order $3^5 13$. Similarly $P_3 = 3^{3+3} L_3(3)$ has no subgroup of order $3^5 13$.

If $A = S_9$, the degree is $12636 = 2^2 3^5 13$ and the relevant maximal factorizations of G have the other factor one of $G_2(3), N_1^+$ and P_3. Now $G_2(3)$ has no exact factorization. Next, $N_1^+ = L_4(3).2$; the only maximal subgroups of $L_4(3)$ of order divisible by 13 are the parabolic subgroups $3^3 L_3(3)$, from which we see there is no subgroup of the required order. The same applies for $P_3 = 3^{3+3} L_3(3)$.

If finally $A \cap L = 2^6.A_7$, the degree is $3^7 13$ and B is a subgroup of P_3. Regarding L as a subgroup N_1 of $P\Omega_8^+(3)$, there is a factorization $P\Omega_8^+(3) = L\,\Omega_8^+(2)$ such that $L \cap \Omega_8^+(2) = 2^6.A_7 = A \cap L$ (see [33, p. 106]). However, we show in Section 11 (see case (a) of the $P\Omega_8^+(3)$ part in (11.10)) that N_1 has no subgroup B which is regular on the coset space $P\Omega_8^+(3)/\Omega_8^+(2)$, so there is no regular subgroup B in the case under current consideration.

8 Proof of Theorem 1.1: orthogonal groups of minus type

In this section we prove Theorem 1.1 in the case where G has socle $L = P\Omega_{2m}^-(q)$ $(m \geq 4)$.

Suppose $G = AB$, $A \cap B = 1$ and A max G. By [33] and Lemma 2.6, one of the following holds:

(8.1) $A = N_1$;

(8.2) $A = P_1$ or N_2^+ $(q = 4)$, $B \leq N_G(SU_m(q))$ (m odd);

(8.3) $A = N_G(SU_m(q))$ (m odd), $B \leq P_1$, N_1 or N_2^+;

(8.4) $A = N_G(\Omega_m^-(q^2)$ (m even, $q = 2$ or 4), $B \leq N_1$;

(8.5) $L = \Omega_{10}^-(2)$.

Case (8.1) Here $G = BN_1$ and $|B| = |G : N_1| = \frac{1}{(2,q-1)} q^{m-1}(q^m + 1)$. Moreover B is given by Lemma 4.4, from which we check that the only possibility is $m = 4, q = 2$ and $B \rhd \Omega_{m/2}^-(q^4) = \Omega_2^-(16)$. However in this case $L = \Omega_8^-(2)$ and it follows from Lemma 2.2 that every involution class in G is represented in N_1, so no regular subgroup occurs.

Case (8.2) If $A = P_1$ then $|B| = |G : A| = (q^m + 1)(q^{m-1} - 1)/(q + 1)$ and we have a factorization $N(SU_m(q)) = B(A \cap N(SU_m(q)) \leq BP_1$. For $m \geq 5$ odd, the only factorization of $U_m(q)$ (or an automorphism group) with P_1 as a factor is $U_9(2) = J_3 P_1$. However, it is easily seen using [9] that J_3 and $J_3.2$

have no subgroups of order $(2^9+1)(2^8-1)/3$. A similar argument handles the case where $A = N_2^+$.

Case (8.3) Here $A = N_G(SU_m(q))$ with $m \geq 5$ odd, and

$$|B| = |G:A| = q^{m(m-1)/2}(q^{m-1}+1)(q^{m-2}-1)\cdots(q^2+1)(q-1). \quad (3)$$

Suppose first that $B \leq P_1$, and write $P = QR$ where Q is the unipotent radical and the Levi subgroup $R \triangleright \Omega_{2m-2}^-(q)$. Then $A \cap P_1$ lies in $P_1(A)$, hence modulo Q we have a factorization $R = \bar{B}\bar{P}_1$ (where bars denote image modulo Q). There are no such factorizations of $\Omega_{2m-2}^-(q)$ or an automorphism group thereof (note $m-1$ is even).

Next suppose that $B \leq N_1$. Then $N_1 = B(A \cap N_1) \leq BN_G(SU_{m-1}(q))$. For q odd there is no such factorization of N_1, so q is even and we have

$$N(Sp_{2m-2}(q)) = BN(SU_{m-1}(q)) \leq BN(\Omega_{2m-2}^+(q)).$$

Clearly $B \not\geq Sp_{2m-2}(q)$ by (3). Hence [33] implies that either $B \leq N(Sp_{2a}(q^b))$ $(ab = m-1, b > 1)$, or $B \leq N(\Omega_{2m-2}^-(q))$ $(q = 2$ or $4)$, or $B \leq N(L_2(17))$ $(m = 5, q = 2)$. The first and third cases are out by (3). In the second case we have a factorization of the form $N(\Omega_{2m-2}^-(q)) = BN_1$. Then [33] forces $B \triangleright \Omega_{2m-2}^-(q)$ or $\Omega_{m-1}^-(q^2)$, neither of which is possible by (3). The same observation rules out the last possibility in (8.3), namely $B \leq N_2^+$.

Case (8.4) In this case $A \cap N_1 \triangleright \Omega_{m-1}(q^2)$, so the factorization $N_1 = B(A \cap N_1)$ gives

$$N_G(Sp_{2m-2}(q)) = BN(\Omega_{m-1}(q^2)) \leq BP_1.$$

As $m-1 \geq 3$ is odd, Lemma 3.1 now implies that either $B \triangleright Sp_2a(q^b)$ $(ab = m-1)$ or $m = 4$ and $B \triangleright G_2(q)$. Since $|B| = |G:A|$, arithmetic shows that only the second possibility can hold.

If $q = 4$ then from [25, 4.3.16] we have $A \cap L = \Omega_4(16).2$, while $B \cap L = G_2(4)$, so $|L|_2/(|A|_2|B|_2) = 2^3$. This is impossible as $|G:L|$ divides $|\mathrm{Out}(L)| = 4$.

Finally, if $q = 2$ then our potential exact factorization of G is $\Omega_8^-(2).2 = (L_2(16).4)\ (G_2(2) \times 2)$. However, we claim that this is not a factorization, and prove this by showing that the subgroups $L_2(16)$ and $G_2(2)$ meet the same involution class of L. To see this, we refer to [9, p.88]. All classes of involutions in L meet $Sp_6(2)$. The irreducible character of degree 34 splits as a sum of two irreducibles of $Sp_6(2)$, one of degree 7 and the other of degree

27. We deduce that the class $2B$ of L contains involutions from both classes $2A$ and $2C$ in $Sp_6(2)$. From the permutation character we see that these involutions are not contained in $G_2(2)$. On the other hand, the other two classes of involutions in L therefore have to be represented in $G_2(2)$. Next, considering possible restrictions of the character of degree 34 to $L_2(16)$, we see that the value on involutions there has to be 2, so the class in L to which these belong is either $2A$ or $2C$ (in fact it is the latter). This establishes the claim.

Case (8.5) Here $L = O_{10}^-(2)$. The factors in L are P_1 and A_{12}, intersecting in a subgroup $(S_4 \times S_8)^+$ of A_{12}. The index of A_{12} in L is $2^{11}.51$, whereas it is quite easy to see (cf. [9, p. 89]) that any subgroup of $O_8^-(2)$ (and hence P_1) of order divisible by 51 involves $L_2(16)$ and hence has order divisible by 5. On the other hand, if $A = P_1$ of index 495, then A_{12} does not have a suitable exact factorization.

9 Proof of Theorem 1.1: some special actions of symplectic and orthogonal groups

In this section we prove Theorem 1.1 in the following two special cases:

L	Ω	$\|\Omega\|$
$Sp_{2m}(q)$ (q even, $m \geq 2$)	$L/O_{2m}^-(q)$	$\frac{1}{2}q^m(q^m-1)$
$P\Omega_{2m}^+(q)$ ($m \geq 4$)	L/N_1	$\frac{1}{(2,q-1)}q^{m-1}(q^m-1)$

(4)

It will turn out that the main candidates for regular subgroups in these cases contain normal subgroups $L_2(q^{m/2})$. It is convenient to begin by classifying such subgroups.

Proposition 9.1 *Let L, Ω be as in (4). Suppose m is even, and let $S \leq L$ with $S \cong L_2(q^{m/2})$ and S semiregular on Ω. If q is odd, assume that S is contained in a parabolic P_m or P_{m-1} of L. Then the following hold.*

(i) *S is a factor of $L_2(q^{m/2}) \times L_2(q^{m/2}) = P\Omega_4^+(q^{m/2}) < L$; conversely, such a factor is indeed semiregular on Ω.*

(ii) *S is contained in a Levi subgroup of a parabolic subgroup P_m (or P_{m-1}in the orthogonal case) of L.*

(iii) *$C_L(S) \cong L_2(q^{m/2})$.*

(iv) *If q is even, u is an involution in $C_L(S)$ and s is an involution in S, then su fixes a point of Ω.*

Proof (A) Suppose first that q is even. Let $V = V_{2m}(q)$ be the natural module for L. Let $t \in S$ be an element of order 3 so that V is completely reducible as $\langle t \rangle$-module. If $W = C_V(t)$ is nonzero then it is non-degenerate and so t lies in $Sp(W^\perp) \times 1^W$ or $\Omega(W^\perp) \times 1^W$, from which it follows easily that t fixes a point of Ω, contrary to our semiregularity assumption. Hence $C_V(t) = 0$.

By Lemma 2.5, the $\mathbb{F}_q S$-composition factors of V are sums of field twists of tensor products $V_2 \otimes V_2^{(2^{i_1})} \otimes \ldots \otimes V_2^{(2^{i_l})}$, realised over $\mathbb{F}_q$, where V_2 is the natural module for S. If $l \geq 1$ then t has nonzero fixed point space on such a tensor product. It follows that $l = 0$ and the $\mathbb{F}_q S$-composition factors of V are m-dimensional modules of the form $V_2 \oplus V_2^{(q)} \oplus \ldots \oplus V_2^{(q^{m/2-1})}$, realised over $\mathbb{F}_q$.

Thus S has two m-dimensional composition factors on V of the above form. In particular S fixes an m-dimensional subspace U of V, and U is either totally singular or non-degenerate.

Suppose U is non-degenerate. Now S fixes an $\mathbb{F}_{q^{m/2}}$-symplectic form $[\,,\,]$ on $V_2 = V_2(q^{m/2})$, unique up to $\mathbb{F}_{q^{m/2}}$-scalar multiplication. Identifying the vectors in U with those of V_2, we see that S fixes the $\mathbb{F}_q$-symplectic form on U defined by $(u, v) = \mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^{m/2}}}[u, v]$. If we take an involution $s \in S$ sending $e \to e$, $f \to f + e$ for some $\mathbb{F}_{q^{m/2}}$-basis e, f of V_2, then s has Jordan form J_2^m on V, and satisfies $(v, s(v)) \neq 0$ for some $v \in V$ (for example take $v = \lambda f$ ($\lambda \in \mathbb{F}_{q^{m/2}}$), where $\mathrm{Tr}(\lambda^2[e, f]) \neq 0$). Hence by Lemma 2.1, some conjugate of s fixes a point of Ω, a contradiction.

Hence U, and indeed every S-invariant m-subspace of V, is totally singular. In particular $S < L_U = P_m$, a parabolic subgroup of L. Write $P_m = QR$, where Q is the unipotent radical and $R \cong GL_m(q)$ is a Levi subgroup. Then Q is elementary abelian, and has the structure of an $\mathbb{F}_q R$-module, with composition factors V_m, $\wedge^2 V_m$, if $L = Sp_{2m}(q)$, and just $\wedge^2 V_m$ if $L = P\Omega_{2m}^+(q)$ (where V_m denotes a natural module for R).

The Levi subgroup R has a subgroup $T \cong SL_2(q^{m/2})$ acting as above on V_m (namely, as $V_2 \oplus V_2^{(q)} \oplus \ldots \oplus V_2^{(q^{m/2-1})}$, realised over $\mathbb{F}_q$). Observe that this subgroup T acts semiregularly on Ω: for semisimple elements of T are clearly semiregular, while an involution $t \in T$ acts on V with Jordan form J_2^m and satisfies $(v, t(v)) = 0$ for all $v \in V$, hence is fixed point free on Ω by Lemmas 2.1 and 2.2.

We next aim to prove that

$$S \text{ is } Q\text{-conjugate to } T. \tag{5}$$

We first claim that in P_m there are at most two conjugacy classes of subgroups $SL_2(q^{m/2})$ which project to T (via the canonical map $QR \to R$). If $L = P\Omega^+_{2m}(q)$, then as an $\mathbb{F}_q T$-module we have

$$Q \downarrow T = \wedge^2 V_m \downarrow T \cong \sum_{i<j} V_2^{(q^i)} \otimes V_2^{(q^j)} + \mathrm{triv}_{m/2}$$

(realised over $\mathbb{F}_q$). Hence from Lemma 2.5(ii) we see that $H^1(T, Q) = 0$, whence the semidirect product QT has just one class of complements to Q, giving the claim. If $L = Sp_{2m}(q)$ this is no longer the case: here we have

$$Q \downarrow T = \sum_{i=1}^{m/2} V_2^{(q^i)} \,/\, \sum_{i<j} V_2^{(q^i)} \otimes V_2^{(q^j)} \,/\, \mathrm{triv}_{m/2}$$

(realised over $\mathbb{F}_q$). Hence we see from Lemma 2.5(ii) that $H^1(T, Q)$ has dimension at most $m/2$ over $\mathbb{F}_q$, arising from the fact that $H^1(T, V_2^{(q^i)})$ has dimension 1 for each i. As a module over $\mathbb{F}_q$ for a subgroup $GL_2(q^{m/2})$ of R containing T, $\sum_i H^1(T, V_2^{(q^i)})$ is of the form $V_1 + V_1^{(q)} + \ldots + V_1^{(q^{m/2-1})}$ realised over $\mathbb{F}_q$, where V_1 is a 1-dimensional module over $\mathbb{F}_{q^{m/2}}$ for $GL_2(q^{m/2})$. In particular $GL_2(q^{m/2})$ acts transitively on the nonzero elements of this module, and it follows that there are at most two classes of complements to Q in the semidirect product QT, which establishes our claim in this case also.

We now deduce the assertion (5). If $L = P\Omega^+_{2m}(q)$ then as shown above, the semidirect product QT has just one class of complements to Q. Since QS is conjugate to QT, (5) follows in this case.

Now assume $L = Sp_{2m}(q)$. We first produce a complement to Q in QT which is not conjugate to T. Let X be a non-degenerate m-subspace of V, and let $S_1 \cong SL_2(q^{m/2})$ be a subgroup of L fixing X and $X^\perp$, such that

$$X \downarrow S_1 \cong X^\perp \downarrow S_1 \cong \sum_{i=0}^{m/2-1} V_2^{(q^i)}$$

(realised over $\mathbb{F}_q$). If $\phi : X \to X^\perp$ is an S_1-isomorphism, then S_1 fixes the subspace $W = \{x + \phi(x) \; x \in X\}$, which is a totally singular m-space. Hence we may take $S_1 \leq P_m$. Replacing S_1 by a suitable P_m-conjugate, we may assume that $S_1 \leq QT$. Further, S_1 is not conjugate to T, since it follows from the above observations that an involution in T is fixed point free on Ω, while an involution in S_1 is not.

It now follows that our subgroup S is Q-conjugate to either T or S_1. However, as just noted, S_1 is not semiregular on Ω. Hence S is conjugate to T. This establishes (5), and also proves conclusion (ii) and the last part of (i) of the proposition.

Now consider a subgroup $\Omega_4^+(q^{m/2}) < \Omega_{2m}^+(q) \leq L$. Write $\Omega_4^+(q^{m/2}) = T_1 \times T_2$ with $T_i \cong SL_2(q^{m/2})$. This acts on $V_4(q^{m/2})$ as a tensor product of two 2-dimensional spaces, say $V_1 \otimes V_2$. Then for $v \in V_2$, the subspace $V_1 \otimes v$ is a totally singular m-space in V fixed by T_1, and it follows that T_1 fixes a pair of complementary totally singular m-spaces, hence lies in a Levi subgroup $GL_m(q)$ of a parabolic P_m. Thus we see that S is conjugate to T_1, proving (i).

To prove (iii), let P be a Sylow 2-subgroup of $C_L(T_1)$. Then $P \times T_1$ lies in a parabolic subgroup of L, which must be P_m. Hence $P \leq C_{P_m}(T_1)$, whence $P = C_Q(T_1)$. The composition factors of $Q \downarrow T_1$ are given above, and there are at most $m/2$ trivial ones, whence $|P| \leq q^{m/2}$. Since T_2 lies in $C_L(T_1)$, it follows that $|P| = q^{m/2}$. Moreover the composition factors of T_1 on $V \otimes \bar{\mathbb{F}}_q$ are all 2-dimensional and have multiplicity 2. Hence we see that $C_L(T_1) = T_2$, giving (iii).

Finally we establish (iv). As above take $T_1 \times T_2$ to act on $V_1 \otimes V_2$, a tensor product of 2-dimensional spaces over $\mathbb{F}_{q^{m/2}}$. Let T_i fix a symplectic form $(\ ,\ )_i$ on V_i, and let e_i, f_i be a basis of V_i with $(e_i, f_i)_i = 1$. Then $T_1 \times T_2$ fixes the quadratic form Q_0 on $V_1 \otimes V_2$ which has associated bilinear form $[\ ,\ ]$ equal to the product of $(\ ,\ )_1$ and $(\ ,\ )_2$, and satisfies $Q_0(v_1 \otimes v_2) = 0$ for all $v_i \in V_i$ (see [25, p.127]). For $i = 1, 2$, let $t_i \in T_i$ be the involution which sends $e_i \to e_i$, $f_i \to e_i + f_i$. Then the involution $t_1 t_2$ sends

$$f_1 \otimes f_2 \to e_1 \otimes e_2 + e_1 \otimes f_2 + f_1 \otimes e_2 + f_1 \otimes f_2.$$

Hence $t_1 t_2$ acts on $V_1 \otimes V_2$ with Jordan form J_2^2, and if we write $v = f_1 \otimes f_2$ then $[\lambda v, t_1 t_2(\lambda v)] = \lambda^2$ for $\lambda \in \mathbb{F}_{q^{m/2}}$. Now regarding $V_1 \otimes V_2$ as the $2m$-dimensional space over $\mathbb{F}_q$ with symplectic form $(\ ,\ ) = \mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^{m/2}}}[\ ,\ ]$, we see that $t_1 t_2$ acts on V as J_2^m and, taking $u = \lambda v$ with $\mathrm{Tr}(\lambda^2) \neq 0$, we have $(u, t_1 t_2(u)) \neq 0$. Hence $t_1 t_2$ fixes a point of Ω by Lemma 2.1, and (iv) is proved.

(B) Now assume that q is odd, so that $L = P\Omega_{2m}^+(q)$ and $\Omega = L/N_1$. Again write $V = V_{2m}(q)$. Let $\hat{S}$ be the preimage of S in $\hat{L} = \Omega_{2m}^+(q)$. If t is an involution in $\hat{S}$ then $C_V(t)$ is non-degenerate, so the semiregularity of S on Ω forces $C_V(t) = 0$ and $t = -1_V$. In particular $\hat{S} \cong SL_2(q^{m/2})$.

By hypothesis, $\hat{S}$ is contained in a parabolic $P = P_m$ or P_{m-1} of $\hat{L}$. This parabolic P is the stabilizer of a totally singular m-subspace W of V. As before write $P = QR$, where Q is the unipotent radical and $R \leq GL_m(q)$ is a Levi subgroup.

Consider the action of $\hat{S} \cong SL_2(q^{m/2})$ on the m-space W. This action is realised over $\mathbb{F}_q$, so the set of composition factors of $\hat{S}$ on W is invariant under a Frobenius q-power morphism. Simple arithmetic shows that the only possible sets of composition factors are $\{V_2^{(q^i)} : 0 \leq i \leq \frac{m}{2} - 1\}$ and $\{(V_2 \otimes V_2^{(q_0)})^{(q^i)} : 0 \leq i \leq \frac{m}{4} - 1\}$, where V_2 is the natural 2-dimensional module for $\hat{S}$ and q_0 is a power of p. In fact the latter set is impossible, as $Z(\hat{S})$ acts trivially on $V_2 \otimes V_2^{(q_0)}$, whereas we showed above that it must act as $\langle -1_V \rangle$ on V. It follows that

$$W \downarrow \hat{S} \cong \sum_{1}^{m/2-1} V_2^{(q^i)},$$

realised over $\mathbb{F}_q$.

We next establish that $\hat{S}$ acts completely reducibly on V. Assume for a contradiction that this is not the case. As an $\hat{S}$-module, $V/W \cong W^* \cong \sum_1^{m/2-1} V_2^{(q^i)}$, so it must be the case that $\mathrm{Ext}_{\hat{S}}(V_2, V_2^{(q^i)}) \neq 0$ for some i. By [1, 4.5], for this to be the case we must have $q^i = 3$, and $V \downarrow \hat{S}$ the sum of field twists of a 4-dimensional indecomposable with composition factors $V_2, V_2^{(3)}$. Such an indecomposable can be viewed as the space of homogeneous polynomials of degree 3 in two variables or its dual, from which we see that the action of an element $u \in \hat{S}$ of order 3 has Jordan form (J_3, J_1). Hence the action of u on the whole of V is $(J_3^{m/2}, J_1^{m/2})$. However, such an element fixes pointwise a non-degenerate subspace of dimension $m/2$ (see [42, p.38]), and hence fixes a point of Ω, contradicting the semiregularity of S.

Hence $V \downarrow \hat{S}$ is completely reducible, and is $\sum_1^{m/2-1} V_2^{(q^i)} + \sum_1^{m/2-1} V_2^{(q^i)}$. In particular $\hat{S}$ fixes an m-subspace W' of V such that $V = W \oplus W'$. Assume W' is non-degenerate, so that $\hat{S} \leq \Omega(W') \cong \Omega_m^{\epsilon}(q)$. Consideration of primitive prime divisors of $q^m - 1$ shows that for $|SL_2(q^{m/2})|$ to divide $|\Omega_m^{\epsilon}(q)|$ we must have $4|m$ and $\epsilon = -$. However in this case $\Omega_m^-(q)$ does not contain $-I_m$ (see [25, 2.5.13]), giving a contradiction as $\hat{S}$ contains -1_V. It follows that W' is totally singular. Thus $\hat{S}$ fixes the complementary totally singular m-spaces W, W', and hence $\hat{S}$ lies in a Levi subgroup of P, giving conclusion (ii) of the lemma.

Finally, conclusions (i) and (iii) are proved by similar arguments to those given above for these in part (A) of this proof. ■

Next we establish the existence of the examples in Table 16.1 for this case (i.e. L, Ω as in (4)).

Proposition 9.2 *Regular subgroups B of G exist in each of the following cases:*

G	G_α	B
$Sp_4(4).2$	$O_4^-(4).2$	S_5
$Sp_8(2)$	$O_8^-(2)$	S_5
$\Omega_8^+(2)$	N_1	S_5
$\Omega_8^+(4).2$	N_1	$L_2(16).4$

where in lines 1 *and* 4*, G/L is generated by an involutory field automorphism. Moreover, in each case the subgroup B' is unique up to G-conjugacy.*

Proof First consider the last two lines. Here $L = \Omega_8^+(q)$ with $q = 2$ or 4. By Lemma 9.1 there is a subgroup $S = SL_2(q^2)$ of a Levi $GL_4(q)$ in L which acts semiregularly on Ω. In fact there is a subgroup $S.2 = SL_2(q^2).2$ in this $GL_4(q)$, and any outer involution t of this has Jordan form J_2^4 on $V = V_8(q)$ and satisfies $(v, t(v)) = 0$ for all $v \in V$ (since $GL_4(q)$ fixes a pair of complementary totally singular 4-spaces), and hence t is fixed point free on Ω by Lemma 2.1. It follows that this subgroup $S.2$ is semiregular on Ω. For $q = 2$ this gives a regular subgroup $B \cong S_5$, as required. For $q = 4$, adjoin a field automorphism τ to L. Then the normalizer of S in $G = L\langle\tau\rangle$ contains $S.4 = L_2(16).4$. If this intersects N_1 nontrivially, the intersection must have order 2. However elements in $L_2(16).4 \setminus L_2(16).2$ have order divisible by 4, so this is not possible, and it follows that this subgroup $L_2(16).4$ is regular on Ω, giving the example in line 4 of the table in the conclusion.

Observe that the action of $\Omega_8^+(2)$ on N_1-spaces is contained in the action of $Sp_8(2)$ on the cosets of $O_8^-(2)$, and hence the latter also has a regular subgroup S_5.

Now consider line 1. Let $G = Sp_4(4).2$. By Lemma 9.1 there is a semiregular subgroup $S = SL_2(4)$. Its normalizer in G contains a subgroup S_5. This must intersect $G_\alpha = L_2(16).4$ trivially, since as above, elements of $G_\alpha \backslash L$ have order divisible by 4. Hence this S_5 is regular.

Finally, the uniqueness statement in the proposition follows from Proposition 9.1.

■

Remark The proof shows that the indicated outer automorphisms of L are necessary in lines 1 and 4 of the table in 9.2, hence the $*$ in the corresponding entries of Table 16.1.

Now we embark upon the proof of Theorem 1 for the special actions given in (4). Let G, L, Ω be as in (4), and suppose $B < G$ acts regularly on Ω.

Lemma 9.3 *One of the following holds:*

(i) *m is even and B has a normal subgroup $S \cong L_2(q^{m/2})$, where S is contained in a Levi subgroup $SL_m(q)/\langle -1\rangle$ in L;*

(ii) *$(m,q) = (4,3)$, B lies in a parabolic subgroup P_i ($i = 3$ or 4) of G, and $B \triangleright A_5$, where this A_5 lies in a Levi subgroup $L_4(3)$ of P_i.*

Proof We know that $|B| = \frac{1}{2}q^m(q^m-1)$ or $\frac{1}{(2,q-1)}q^{m-1}(q^m-1)$, according as $L = Sp_{2m}(q)$ or $P\Omega^+_{2m}(q)$. Moreover B satisfies the conclusion of Lemma 4.6 or 4.5, respectively. It follows by arithmetic that one of the following holds:

(α) $B \triangleright L_2(q^{m/2})$ with q even or $(m,q) = (4,3)$;

(β) $B \le P_m$ (or P_{m-1} in the orthogonal case), and modulo the unipotent radical B induces a subgroup of $\Gamma L_m(q)$ which is transitive on 1-spaces.

Consider case (α). If q is even then conclusion (i) holds by Proposition 9.1. Now assume $(m,q) = (4,3)$ and $B \triangleright L_2(9) = A_6$. We have $|B| = 1080$, hence $B = 3 \times A_6$, and so B lies in a maximal parabolic P, which must be P_3 or P_4 (since $G = BN_1$). Hence conclusion (i) holds by 9.1 again.

Now consider case (β). Let $P_m = QR$ as in the proof of Proposition 9.1, and let $\bar{B}$ denote the subgroup of $\Gamma L_m(q)$ induced by B. Then $\bar{B}$ is given by Lemma 3.1. Since $|B| = |\Omega|$ is as in (4), one of the following holds:

(a) $\bar{B} \triangleright L_2(q^{m/2})$;

(b) $\bar{B} \triangleright L_2(13)$ with $(m,q) = (6,3)$;

(c) $\bar{B} \triangleright A_5$ or $\bar{B} \le 2^4.S_5$ with $(m,q) = (4,3)$;

(d) $\bar{B} \le \Gamma L_1(q^m)$.

Consider (a). Since $|B|_p < q^m$, $\bar{B}$ must act trivially on $B \cap Q$, and hence the preimage of $L_2(q^{m/2})$ in B is a central extension of $B \cap Q$ by $L_2(q^{m/2})$. Now the Schur multiplier of $L_2(q^{m/2})$ is a p'-group, with the exception of

$L_2(4)$ and $L_2(9)$ (see [16, 6.1]). Therefore, apart from these exceptions, we have $B \geq L_2(q^{m/2})$, and conclusion (i) now follows by Proposition 9.1. The exceptional possibilities are that B contains a cover $2.L_2(4)$ or $3.L_2(9)$ (with $m = 4$, $q = 2$ or 3). However, there is no such cover in P_m in these cases: for example, when $q = 2$ we have $P_m = P_4 = 2^6.L_4(2)$ or $2^{4+6}.L_4(2)$ according as $L = \Omega_8^+(2)$ or $Sp_8(2)$. The group $\bar{B}$, being transitive on 1-spaces, is an $L_2(4)$ centralizing an element of order 3 in $L_4(2)$, hence acting completely reducibly on 2^6 as $2^2 \oplus 2^4$. The derived group of $2^6.\bar{B}$ is therefore $2^4.\bar{B}$, which does not contain a cover $2.L_2(4)$ as $\bar{B}$ is fixed point free on 2^4. The argument for $q = 3$ is similar.

In case (b) the fact that $|B| = \frac{1}{2}3^5(3^6 - 1)$ forces $B = 3^4.L_2(13)$. We have $Q = \wedge^2 V_6(3)$ as a module for $R' = L_6(3)$, and hence using [20] we see that $Q \downarrow L_2(13)$ has composition factors of orders $3^7, 3^7$ and 3. Hence P_6 has no subgroup $3^4.L_2(13)$, a contradiction.

Now consider (c). Here $|B| = 1080$ and $B \leq P_i \leq 3^6.L_4(3).D_8$, where $i \in \{3, 4\}$. If $|\bar{B}|_3 = 1$ then $|B \cap Q| = 3^3$. However since B has an element of order 5, there is no B-invariant subgroup of order 3^3 in Q, so this is impossible. Hence $|\bar{B}|_3 = 3$, $\bar{B} \rhd A_5$ and $B \cap Q = 3^2 = C_Q(A_5)$. Since the Schur multiplier of A_5 has $3'$-order, it follows that $B \rhd A_5$. Arguing as in part (B) of the proof of Proposition 9.1, we see that this A_5 lies in a Levi subgroup of P_i (using [26, Lemma 1] instead of [1] for the relevant fact about Ext groups). Hence conclusion (ii) of the lemma holds.

Finally, consider (d), in which $\bar{B} \leq \Gamma L_1(q^m)$. Assume first that $(m, q) \neq (6, 2)$, so that B contains an element t of prime order q_m (a primitive prime divisor of $q^m - 1$). The non-trivial composition factors of $Q \downarrow \langle t \rangle$ have order q^m; in addition we have $|C_Q(t)| = 1$ or $q^{m/2}$, according as m is odd or even, respectively. Since $|B|_p < q^m$, it follows that $B \cap Q \leq C_Q(t)$, and so $m \log_p q$ is divisible by $|B|_p/|C_Q(t)|$. Hence one of the following holds:

$$\begin{aligned} &m = 2,\ q = 4 \text{ or } 16 \\ &m = 4,\ q = 2, 4 \text{ or } 16 \\ &m = 8,\ q = 2. \end{aligned}$$

In the $m = 2$ case we have $L = Sp_4(q)$ and $B \cap L \leq N_{P_2}(t) = [q.(q-1)] \times [(q+1).2] \leq L_2(q) \times L_2(q) = \Omega_4^+(q)$. By Proposition 9.1(iv), no involution from the second factor can be present in B. Hence for $q = 16$ we have $B \leq ([q.(q-1)] \times (q+1)).4$, whereas $|B|_2 = 2^7$, a contradiction. And for $q = 4$ we have $G = L.2$ and $B = (2^2.3 \times 5).2$; however, any 2-element in the outer coset of this group would have to have order 4, since $N_{L_2(4).2}(5) = 5.4$, so this is also impossible.

In the $m = 4$ case, we similarly have $B \cap L \leq ([q^2.(q^2-1)] \times (q^2+1)).2 \leq \Omega_4^+(q^2)$, and again any outer 2-element must have order greater than 2, leading to a contradiction. The $m = 8$ case yields to an entirely similar argument.

To complete the proof, observe that in the excluded case $(m, q) = (6, 2)$ we take $t \in B$ to be an element of order 7; then all composition factors of $Q \downarrow \langle t \rangle$ have order 2^3. This yields a contradiction since $|B|_2 = 2^5$. ■

Lemma 9.4 *q is even.*

Proof Suppose q is odd. Then $L = P\Omega_{2m}^+(q)$ $(m \geq 4)$ and $\Omega = L/N_1$. Say N_1 is the stabilizer of a 1-space $\langle w \rangle$ with $(w, w) = 1$.

Assume first that case (i) of Lemma 9.3 holds. By Lemma 9.1, the normal subgroup $S \cong L_2(q^{m/2})$ of B is a factor of a subgroup $S \times T = L_2(q^{m/2}) \times L_2(q^{m/2}) = P\Omega_4^+(q^{m/2}) < L$, and moreover $C_L(S) = T$. Hence B normalizes $S \times T$. Since $|B|_p = q^{m-1}$ it follows that B contains an element $t_2 \in T$ of order p.

However, we claim that we can choose $t_1 \in S$ of order p such that $t_1 t_2$ fixes a point of Ω. To see this, rewrite $S \times T = T_1 \times T_2$ and take this to act on $V_1 \otimes V_2$, a tensor product of 2-dimensional spaces over $\mathbb{F}_{q^{m/2}}$. Let T_i fix a symplectic form $(\ ,\ )_i$ on V_i, and let e_i, f_i be a basis of V_i with $(e_i, f_i)_i = 1$. Then $T_1 \times T_2$ fixes the symmetric form $[\ ,\ ]$ on $V_1 \otimes V_2$ which is the product of $(\ ,\ )_1$ and $(\ ,\ )_2$, and we may assume the $\mathbb{F}_q$-form $(\ ,\ )$ on V preserved by L to be $\mathrm{Tr}_K^k [\ ,\ ]$, where $K = \mathbb{F}_{q^{m/2}}, k = \mathbb{F}_q$. We may take t_i to send $e_i \to e_i$, $f_i \to \alpha_i e_i + f_i$ for $i = 1, 2$ and some $\alpha_i \in \mathbb{F}_{q^{m/2}}$. Then $t_1 t_2$ fixes the vector

$$v = \alpha_1 e_1 \otimes f_2 - \alpha_2 f_1 \otimes e_2.$$

Now $[v, v] = 2\alpha_1\alpha_2$, and so for a suitable choice of α_1 (recall that we can choose t_1 to be any element of order p in S), we have $(v, v) = \mathrm{Tr}_K^k [v, v] = 1$, so the $\mathbb{F}_q$-1-space spanned by v is in Ω and is fixed by $t_1 t_2 \in B$, as claimed. This contradicts the fact that B acts semiregularly on Ω.

Finally, consider case (ii) of Lemma 9.3. As in the fifth paragraph of the proof of that lemma (case (c)), we have $B \cap Q = C_Q(A_5) = 3^2$, and the subgroup $3^2 \times A_5$ of B lies in a subgroup $A_6 \times A_6 = P\Omega_4^+(9) < L$. Then B contains an element $t_1 t_2$, where t_1, t_2 are elements of order 3 in the two factors A_6, and as above, this element fixes a point of Ω, which is a contradiction. ■

At this point we can complete the proof of Theorem 1 for the actions in (4). Let G, L, Ω be as in (4), and suppose $B < G$ is regular on Ω. By Lemmas 9.3 and 9.4, m and q are even, and B has a normal subgroup $S \cong L_2(q^{m/2})$. Moreover, S satisfies (i)-(iv) of Proposition 9.1.

Let $T = C_L(S)$, so $T \cong L_2(q^{m/2})$ by Proposition 9.1(iii). Now $|B|_{2'} = q^m - 1 = |S|_{2'}$, while $|B \cap T|_2 = 1$ by Proposition 9.1(iv). It follows that $B \cap T = 1$. Since S is centralized by no nontrivial field automorphism of L, we have $C_G(S) = C_L(S) = T$, whence $C_B(S) = 1$. Consequently B/S has order dividing $|\mathrm{Out}(S)| = \frac{m}{2}\log_2 q$. Since $|B/S| = \frac{1}{2}q^{m/2}$ if $L = Sp_{2m}(q)$, and $|B/S| = q^{m/2-1}$ if $L = \Omega^+_{2m}(q)$, this forces one of the following to hold:

$$\begin{array}{l} L = Sp_{2m}(q) \,:\, m = 2, q = 4 \text{ or } m = 4, q = 2 \\ L = \Omega^+_{2m}(q) \,:\, m = 4, q = 2 \text{ or } 4. \end{array}$$

In all these cases examples of regular subgroups B exist, and are unique up to conjugacy, by Proposition 9.2. Finally, we see using Proposition 9.1(iv) that there are no further examples of regular subgroups.

This completes the proof of Theorem 1 for the actions in (4).

10 Proof of Theorem 1.1: remaining symplectic cases

In this section we prove Theorem 1.1 in the case where G has socle $L = PSp_{2m}(q)$ ($m \geq 2$, $(m,q) \neq (2,2)$).

Suppose $G = AB$, $A \cap B = 1$ and A max G. By [33] and Lemma 2.6, one of the following holds:

(10.1) $A = N_G(\Omega^\epsilon_{2m}(q))$ (q even, $\epsilon = \pm$);

(10.2) $A = P_1$;

(10.3) $A = N_G(PSp_{2a}(q^b))$, $B \leq P_1$ ($ab = m$, b prime);

(10.4) $A = N_G(PSp_{2a}(q^b))$, $B \leq N_G(\Omega^\epsilon_{2m}(q))$ (q even, $ab = m$, b prime);

(10.5) $A = P_m$, $B \leq N_G(\Omega^-_{2m}(q))$ (q even);

(10.6) $A = N_G(Sp_m(q) \wr S_2)$, $B \leq N_G(\Omega^-_{2m}(q))$ (m even, q even);

(10.7) $A = N_2$, $B \leq N_G(Sp_m(q^2))$ ($m \geq 4$ even, $q = 2$ or 4);

(10.8) $A = N_G(Sp_m(q^2))$, $B \leq N_2$ ($m \geq 4$ even, $q = 2$ or 4);

(10.9) $A = N_G(Sp_{2m}(q^{1/2}))$, $B \leq N_G(\Omega^-_{2m}(q))$ ($q = 4$ or 16);

(10.10) $m = 2$, $A = N(Sz(q))$ or $B \leq N(Sz(q))$ ($q = 2^{2a+1} \geq 8$);

(10.11) $m = 3$, $A = N(G_2(q))$ or $B \leq N(G_2(q))$ (q even);

(10.12) $L = PSp_4(3)$, $PSp_6(3)$ or $Sp_8(2)$.

Case (10.1) For $\epsilon = -$ this case has been handled in Section 9. So assume $\epsilon = +$. Then $A = N_G(\Omega^+_{2m}(q))$ and $|B| = \frac{1}{2}q^m(q^m+1)$. By Lemma 2.3, A contains representatives of all involution classes in L, and hence, as B is regular on Ω, B can contain no such involutions; in other words, $|B \cap L|$ is odd. It follows that $|B|_2 = \frac{1}{2}q^m$ divides $|G : L|$, hence divides $\log_2 q$. This is impossible.

Case (10.2) Here $A = P_1$, $|B| = (q^{2m}-1)/(q-1)$, and by Lemma 3.1 we have $B \leq \Gamma L_1(q^{2m})/\langle -1 \rangle$. Now $\Gamma L_1(q^{2m}) \cap Sp_{2m}(q) = (q^m+1).2m$ (see for example the proof of [25, 4.3.15]), and hence $(q^{2m}-1)/(q-1)$ must divide $(q^m+1).2m \log q$. This forces $m = 2, q = 3$. In this case $L = PSp_4(3) \cong U_4(2)$, which was handled in (6.3).

Case (10.3) Here $B \leq P_1$ and $A = N_G(PSp_{2a}(q^b))$ ($ab = m$, b prime), and we have

$$|B| = |L : A| = \frac{1}{b} q^{m(m-a)} \prod_{i \leq m-1, i \neq kb} (q^{2i}-1). \tag{6}$$

Write $P_1 = QR$ where Q is the unipotent radical and R a Levi subgroup, so $R \rhd Sp_{2m-2}(q)$. As usual set $\bar{B} = BQ/Q$. If $P_1 = G_{\langle v \rangle}$ then $A \cap P_1$ stabilizes the 1-space spanned by v over $\mathbb{F}_{q^b}$, and hence we have a factorization $R = \bar{B}P_{b-1}$. By [33] this forces one of the following to hold:

(1) $\bar{B} \rhd Sp_{2m-2}(q)$

(2) $b = m > 2$

(3) $b = 2$.

Consider first case (1). Here (6) forces $b = m$, and $|B|/|Sp_{2m-2}(q)| = q^{m-1}/m$. Hence as m is prime, $m = p$. Moreover $Sp_{2m-2}(q)$ has composition factors on Q of orders q and q^{2m-2}, and so $B \cap Q \leq Q_0$, where $Q_0 = C_Q(Sp_{2m-2}(q))$, a group of order q. Thus q^{m-1}/m divides $q \log q$. If $m = 2$ then $p = 2$ and $A = N_G(Sp_2(q^2))$ is conjugate under a graph automorphism of L to $N(O_4^-(q))$, a case already handled in Section 9. The only other possibility is that $m = p = 3$, in which case q^2 divides $3q \log q$, forcing $q = 3$, and $A \cap L = PSp_2(27).3$, $B \cap L = Sp_4(3) \times 3$. But then A and B contain conjugate elements of order 3 and Jordan form J_2^3.

For the rest of the proof we may assume that $\bar{B} \ngeq Sp_{2m-2}(q)$.

Consider case (2): $b = m > 2$. Here the factorization $R = \bar{B}P_{m-1}$ implies using [33] that one of the following holds:

(2i) $\bar{B} \leq N(O^-_{2m-2}(q))$, q even

(2ii) $m = q = 3$, $\bar{B} \leq 2^{1+4}.S_5$

(2iii) $m = 3, q = 2$.

In case (2i) we have $B \leq Q.(O^-_{2m-2}(q) \times (q-1)).\log q$, and hence by (6), $q^{m-1} - 1$ divides $m(q-1)\log q$. This forces $m = 3$, $q = 2$ or 8. For $q = 2$ the only possibility for B is $2^4.A_5$, and we claim there is indeed an exact factorization

$$Sp_6(2) = (Sp_2(8).3)\,(2^4.A_5),$$

as in Table 16.1. To prove this claim, we start with the factorization $Sp_6(2) = (Sp_2(8).3)\,O^-_6(2)$ given by [33]. The intersection of the two factors is $O^-_2(8).3$, which is not contained in $\Omega^-_6(2)$, and hence we also have $Sp_6(2) = (Sp_2(8).3)\,\Omega^-_6(2)$, the factors intersecting in $\Omega^-_2(8).3 = 9.3$. Now take $B = 2^4.A_5 = P_1(\Omega^-_6(2)$. Then B is also $P_2(U_4(2))$. From Section 6 we have an exact factorization of $U_4(2)$ which interpreted for $\Omega^-_6(2)$ takes the form $\Omega^-_6(2) = P_1\Omega^-_2(8).3$, and the claim follows.

Finally, for $m = 3, q = 8$ we assert that no example arises: for here the relevant exact factorization must be $Sp_6(8).3 = (Sp_2(8^3).9)\,B$, where $B = (\mathbb{F}_8)^4.(\Omega^-_4(8) \times 7).3$, and B is unique up to P_1-conjugacy. Hence B is the stabilizer of a singular 1-space in $\Omega^-_6(8)$. Since $Sp_6(8) = (Sp_2(8^3).3)\,\Omega^-_6(8)$, with factors intersecting in $\Omega^-_2(8^3).3$, this leads to a factorization $\Omega^-_6(8).3 = P_1\,(\Omega^-_2(8^3).3.3)$. However there is no such factorization, by [33].

Next consider case (2ii): $m = q = 3$, $\bar{B} \leq 2^{1+4}.S_5$. Under the action of a subgroup of order 5 in B, the radical $Q = 3^{1+4}$ contains no invariant 3^4, and hence the only possibility is $B = Q.(2^{1+4}.5.4)$. We claim that there is an example of this form, i.e. an exact factorization

$$PSp_6(3).2 = AB = (PSp_2(27).3.2)\,(3^{1+4}.2^{1+4}.5.4),$$

as in Table 16.1. To see this, observe first that $|A \cap B|_3 = 1$: for the elements of order 3 in A have Jordan form J_2^3 or J_3^2, whereas those in B (hence in Q) do not. Next, $|A \cap B \cap L|_2 = 1$: for involutions in P_1 lift to involutions in $Sp_6(3)$, whereas involutions in the subgroup $PSp_2(27)$ lift to elements of order 4. Finally, $|A \cap B|_2 = 1$ also, since, working in $B/O_{2,3}(B) = 5.4$, we see that every 2-element of $B \cap (L.2\backslash L)$ has order divisible by 4 and has a power which is an involution in L. This proves the existence of the above exact factorization.

Now consider case (2iii): $m = 3, q = 2$. Here the factorization $R = Sp_4(2) = \bar{B}P_2$ implies that $\bar{B} \geq A_5$ by [33]. Moreover $|B| = 2^4 \cdot 60$, so the only possibility is given by the exact factorization $Sp_6(2) = (Sp_2(8).3)\,(2^4.A_5)$, the existence of which was established above. This completes our analysis of case (2).

To complete this subsection (10.3), consider case (3): $b = 2$. Here $m = ab$ is even and

$$|B| = \frac{1}{2}q^{m^2/2}(q^{2m-2}-1)(q^{2m-6}-1)\dots(q^2-1).$$

The factorization $R = \bar{B}P_1$ implies by Lemma 3.1 that one of the following holds:

(3i) $\bar{B} \rhd Sp_{2c}(q^d)$ with $cd = m-1, d \geq 3$

(3ii) $\bar{B} \rhd G_2(q^d)$ with q even, $3d = m-1$

(3iii) $m = 4, q = 3$ and $\bar{B} \rhd SL_2(13)$ $(< Sp_6(3))$

(3iv) $m = 2$, $q \in \{5, 7, 9, 11, 19, 23, 29, 59\}$, $\bar{B} \rhd Q_8$ or $SL_2(5)$

(3v) $\bar{B} \cap Sp_{2m-2}(q) \leq \Gamma L_1(q^{2m-2})$.

In case (3i), the fact that $|B|$ is divisible by $q^{2m-6}-1$ forces $m = 4$ and $\bar{B} \rhd Sp_2(q^3)$. Now B acts on Q with composition factors of order q and q^6. Since $|B|_p = q^8/(2,q)$, it follows that $|B \cap Q|$ divides q. However this means that $|B \cap L|_p \leq q^4$, hence $q^4/(2,q)$ divides $|\mathrm{Out}(L)|$, which is clearly impossible.

Now consider (3ii). Here again the divisibility of $|B|$ by $q^{2m-6}-1$ forces $d = 1$ and $m = 4$, and as above $|B \cap Q|$ divides q. We claim that A and B both contain conjugates of an element of order $q+1$, which will contradict the factorization $G = AB$. To see the claim, consider $G_2(q) < Sp_6(q) < L$. A subgroup $S = SL_2(q)$, generated by long root elements of $G_2(q)$, acts on the natural module V_8 as $V_2^2 + V_1^4$, and hence S has an element s of order $q+1$ acting on V_8 as $(A, A, 1^4)$, where A stands for a 2×2 matrix of order $q+1$. Then B contains a conjugate of s. Moreover, so does A, within a natural subgroup $Sp_2(q^2)$ of $Sp_4(q^2) \lhd A$. This proves the claim.

Next consider (3iii). Here $|B|_2 \leq 2|SL_2(13)|_2 = 2^4$, whereas $|B| = \frac{1}{2}3^8(3^6-1)(3^2-1)$ has 2-part 2^5, a contradiction.

In case (3iv) we have $|B| = \frac{1}{2}q^2(q^2-1)$, and as before $|B \cap Q|$ divides q. Hence q divides $|\bar{B}|$, which is not possible.

Finally consider (3v). We have $|Sp_{2m-2}(q) \cap \Gamma L_1(q^{2m-2})| = (q^{m-1}+1)(m-1) \cdot (2,q)$ (contained in a subgroup $Sp_2(q^{m-1}).(m-1)$ - see the proof of [25, 4.3.15]. Hence $|B|$ divides $2(q^{m-1}+1)(m-1)(q-1)\log q$. This must be divisible by $q^{m-1}-1$, which forces $m=2$. Then $|B| = \frac{1}{2}q^2(q^2-1)$, and as usual $|B \cap Q|$ divides q. Hence $\frac{1}{2}q$ divides $2\log q$, so $q = 4$ or 16 (recall $q \neq 2$ since by assumption $L \neq Sp_4(2) \cong S_6$). Now applying a graph automorphism of $L = Sp_4(q)$ to A and B, we have $A = N(O_4^-(q))$ and $B \leq P_2$. Hence we are done by Section 9.

Case (10.4) Here $A = N_G(PSp_{2a}(q^b))$, $B \leq N_G(\Omega_{2m}^\epsilon(q))$ (q even, $ab = m$, b prime), and $|B|$ is as in (6). There is a factorization

$$N_G(\Omega_{2m}^\epsilon(q)) = B\,N(O_{2a}^\epsilon(q^b)), \tag{7}$$

and $B \not\geq \Omega_{2m}^\epsilon(q)$ (by (6)). Hence by [33], one of the following holds:

(1) $m \geq 4$, $b = 2$, $q = 2$ or 4, and $B \leq N_1$ (or an image of N_1 under triality if $m = 4, \epsilon = +$)

(2) $m \leq 3$.

Consider first case (1). Here $|B| = \frac{1}{2}q^{m^2/2}(q^{2m-2}-1)(q^{2m-6}-1)\ldots(q^2-1)$, so $B \not\geq \Omega_{2m-1}(q)$. From [33] we see that $N_1 \cap O_m^\epsilon(q^2)$ fixes a 1-space of the natural module for $Sp_{2m-2}(q) \cong \Omega_{2m-1}(q)$, and hence (7) leads to a factorization

$$N(Sp_{2m-2}(q)) = BP_1.$$

By Lemma 3.1 together with the fact that $m \geq 4$ is even, it follows that either $B \leq N(Sp_{2c}(q^d)$ ($cd = m-1$, $d \geq 3$), or $m = 4$ and $B \triangleright G_2(q)$. In the former case $|B|_p < \frac{1}{2}q^{m^2/2}$, a contradiction. And in the latter case, we see as in the case (3ii) of (10.3) above, that A and $G_2(q)$ both contain conjugates of an element of order $q+1$, which contradicts the exact factorization $G = AB$.

Now consider case (2): $m \leq 3$. If $m = 2$ we can apply a graph automorphism of L to take $A = N(O_4^-(q))$, and we are done by Section 9. So assume that $m = 3$. Then $|B| = \frac{1}{3}q^6(q^4-1)(q^2-1)$, and (7) gives a factorization $N_G(O_6^\epsilon(q)) = B\,N(O_2^\epsilon(q^3))$. For $q > 2$ there is no possible such factorization, by [33]; neither is there for $q = 2, \epsilon = +$ (note that $O_6^+(2) \cong S_8$). For $q = 2, \epsilon = -$, the only possibility is the factorization arising from $U_4(2) = (9.3)\,P_2$ which we have seen in Section 6, leading to the example

$$Sp_6(2) = (Sp_2(8).3)\,(2^4.A_5),$$

seen in case (2i) of (10.3) above.

Case (10.5) Here $A = P_m$ and $B \leq N_G(\Omega_{2m}^-(q))$ (q even). We have $|B| = |G : A| = \prod_{i=1}^m (q^i+1)$. From [33] we see that $A \cap O_{2m}^-(q)$ fixes a totally singular $(m-1)$-space, and hence we get a factorization

$$N_G(\Omega^-_{2m}(q)) = BP_{m-1}.$$

There is no such factorization for $m \geq 3$, by [33] (note that for $m = 3$ it translates into a factorization of type $U_4(q) = BP_1$). Finally, $m = 2$ is also not possible as $\mathrm{Aut}(L_2(q^2))$ has no subgroup of order $(q^2+1)(q+1)$.

Case (10.6) Here $A = N_G(Sp_m(q) \wr S_2)$ and $B \leq N_G(\Omega^-_{2m}(q))$ (m even, q even), and we get a factorization

$$N_G(\Omega^-_{2m}(q)) = B\,N(O^+_m(q) \times O^-_m(q)).$$

Clearly $B \not\geq \Omega^-_{2m}(q)$, so there is no such factorization for $m \geq 4$, by [33]. And for $m = 2$ we have $|B| = \frac{1}{2}q^2(q^2+1)$, and the above factorization is $N(L_2(q^2)) = B\,N(q^2-1)$, which is not possible for $q > 2$.

Case (10.7) Here $A = N_2$, $B \leq N_G(Sp_m(q^2))$ ($m \geq 4$ even, $q = 2$ or 4), and $|B| = |G : A| = q^{2m-2}(q^{2m}-1)/(q^2-1)$. From [33] we see that $A \cap N_G(Sp_m(q^2))$ normalizes $Sp_2(q) \times Sp_{m-2}(q^2)$, so we get a factorization

$$N_G(Sp_m(q^2)) = B\,N(Sp_2(q) \times Sp_{m-2}(q^2)) \leq BN_2.$$

Hence by [33], one of the following holds:

(1) $q = 2$, $B \leq N(Sp_{m/2}(16))$

(2) $m = 6$, $B \leq N(G_2(q^2))$.

In case (1), repetition of the above considerations yields a factorization $N_G(Sp_{m/2}(16)) = B\,N(Sp_2(4) \times Sp_{m/2-2}(16))$, which implies by [33] that either $m = 12$, $B \leq N(G_2(16))$, or $m = 4$, $B \leq N(17)$. In the latter case $|B|$ cannot be divisible by 5, a contradiction. In the former, as $G_2(16)$ and its automorphism groups have no proper factorizations (see [33, Theorem B]), we have $B \geq G_2(16)$, contrary to the above formula for $|B|$.

In case (2), the factorizations of $G_2(q^2)$ imply that $q = 2$ and $B \triangleright SU_3(4), G_2(2)$ or J_2. None of these are possible by the formula for $|B|$.

Case (10.8) Here $A = N_G(Sp_m(q^2))$, $B \leq N_2$ ($m \geq 4$ even, $q = 2$ or 4), and projecting to the $Sp_{2m-2}(q)$ factor of N_2, we get a factorization

$$N(Sp_{2m-2}(q)) = \bar{B}\,N(Sp_2(q) \times Sp_{m-2}(q^2))$$

where $\bar{B}$ is the projection of B. As in the previous case this forces $m = 4$ and $\bar{B} \triangleright G_2(q)$. However, as in case (3ii) of (10.3) above, A and $G_2(q)$

both contain conjugates of an element of order $q+1$ in G, which gives a contradiction.

Case (10.9) Here $A = N_G(Sp_{2m}(q^{1/2}))$, $B \le N_G(\Omega^-_{2m}(q))$ ($q = 4$ or 16), and

$$|B| = |G : A| = q^{m^2/2} \prod_{i=1}^{m} (q^i + 1). \tag{8}$$

From [33] we have $A \cap O^-_{2m}(q) = O_{2m-1}(q^{1/2}) \times 2$, so there is a factorization

$$N_G(\Omega^-_{2m}(q)) = B\, N(O_{2m-1}(q^{1/2})) \le BN_1.$$

For $m = 2$ or 3, neither $\mathrm{Aut}(L_2(q^2))$ nor $\mathrm{Aut}(U_4(q))$ has a subgroup of the order required by (8). And for $m \ge 4$, the above factorization implies by [33] that either $B \le N(SU_m(q))$ with m odd, or $B \le N(\Omega^-_m(q^2))$ with m even, $q = 4$. Neither of these is possible, again by (8).

Case (10.10) As $Sz(q)$ and its automorphism groups do not have proper factorizations, the only possibility here is that $A = N(Sz(q))$ and $B \le N(O^+_4(q))$ (see [33]). Then $|B| = |G : A| = q^2(q^2-1)(q+1)$. However it is easy to see that there is no subgroup of this order in $N(O^+_4(q))$ ($\le \mathrm{Aut}(L_2(q)^2)$) for $q = 2^{2a+1} \ge 8$.

Case (10.11) As $G_2(q)$ and its automorphism groups do not have proper exact factorizations, we must have $A = N(G_2(q))$. By [33] we have $\Omega^+_8(q) = Sp_6(q)\, N_1$ (where the $Sp_6(q)$ factor acts irreducibly), and the intersection of the two factors is $G_2(q)$. Hence the action of $L = Sp_6(q)$ on the cosets of $G_2(q)$ is contained in that of $\Omega^+_8(q)$ on N_1. The possibilities for regular subgroups of $\Omega^+_8(q)$ in this action are determined in Section 9; they are given in the last two rows of the table in Proposition 9.2. Inspection of the proof of this proposition shows that the subgroups $B = S_5, L_2(16).4$ in these rows lie in an irreducible subgroup $Sp_6(q)$ of $\Omega^+_8(q)$, and hence these examples carry over to this case, and are recorded in Table 16.1.

Case (10.12) We have already dealt with $L = PSp_4(3) \cong U_4(2)$ in Section 6. In the remaining cases L is either $PSp_6(3)$ or $Sp_8(2)$. We consider maximal factorizations of G containing AB which have not already been considered in previous cases.

Let $L = PSp_6(3)$. The maximal factorization of L to be considered here has factors $L_2(13)$ and P_1, intersecting in a subgroup of order 3. If

$A = L_2(13)$ then $G = L$; however P_1 has no subgroup of index 3. And, A cannot be P_1 either, since $L_2(13)$ has no subgroup of index less than 14.

Now let $L = Sp_8(2)$. There are two factorizations to consider here. In one, the factors are S_{10} and $O_8^-(2).2$, intersecting in a subgroup $S_7 \times S_3$. Now S_{10} does not have a suitable exact factorization, so $A = S_{10}$ and B is a proper subgroup of $O_8^-(2).2$. Since 17 divides the order of B, it follows from [9, p. 89] that B is a subgroup of $L_2(16)$, which is clearly impossible by considering the power of 2. In the other factorization, the factors are $L_2(17)$ and $O_8^+(2).2$, intersecting in a subgroup D_{18}. Now $O_8^+(2).2$ has no subgroup of index 18, so $A = O_8^+(2).2$, of index 136. However, $L_2(17)$ does not have a suitable exact factorization, as it has a unique class of involutions.

11 Proof of Theorem 1.1: orthogonal groups of plus type

In this section we prove Theorem 1.1 in the case where G has socle $L = P\Omega_{2m}^+(q)$ $(m \geq 4)$.

Suppose $G = AB$, $A \cap B = 1$ and A max G. By [33] and Lemma 2.6, one of the following holds (if necessary replacing A by its image under some automorphism of L):

(11.1) $A = N_1$;

(11.2) $B \leq N_1$ and $A = P_m$, P_{m-1}, $N_G(SL_m^\epsilon(q))$, $N_G(PSp_2(q) \otimes PSp_m(q))$ (m even, $q > 2$), $N_G(\Omega_m^+(q^2))$ (m even, $q = 2, 4$), or $N_G(\Omega_8^-(q^{1/2}))$ ($m = 4$, q square);

(11.3) $A = N_2^-$ and $B \leq P_m$, P_{m-1} or $N_G(SL_m(q))$ $(q = 2, 4)$;

(11.4) $A = P_1$ and $B \leq N_G(SU_m(q))$ (m even);

(11.5) $A = N_G(SU_m(q))$ and $B \leq P_1$ (m even);

(11.6) $A = N_2^+$ and $B \leq N_G(SU_m(q))$ ($q = 4$, m even);

(11.7) $A = N_G(SU_m(q))$ and $B \leq N_2^+$ ($q = 4$, m even);

(11.8) $L = P\Omega_{16}^+(q)$, $A = N_G(\Omega_9(q))$ and $B \leq N_1$;

(11.9) $L = \Omega_{24}^+(2)$, $A = Co_1$ and $B \leq N_1$;

(11.10) $L = P\Omega_8^+(q)$ $(q = 2, 3, 4)$, and the factorization $G = AB$ is contained in one in the bottom half of [33, Table 4].

Note that when $m = 4$ some apparently missing cases are omitted above because of the presence of the triality automorphism of $L = P\Omega_8^+(q)$ — for example, the case where $A = P_1$, $B \leq \Omega_7(q)$ is in fact included under (11.2), since triality sends P_1 to P_3 or P_4 and sends $\Omega_7(q)$ to N_1; likewise, the cases where $A = N_2^+$ or N_2^-, and $B \leq \Omega_7(q)$, are also under (11.2) as triality sends N_2^+ to $N_G(SL_4(q))$, and N_2^- to $N_G(SU_4(q))$. (For $\varepsilon = +$ or $-$ we write $SL_m^\varepsilon(q)$ for $SL_m(q)$ or $SU_m(q)$ respectively.)

Case (11.1) This has been handled in Section 9.

Case (11.2) Here $B \leq N_1$ and we have a factorization

$$N_1 = B\,(N_1 \cap A). \tag{9}$$

By arithmetic, B does not contain $\Omega_{2m-1}(q)$, so the possibilities are given by the factorizations of $\Omega_{2m-1}(q)$ in [33].

If $A = P_m$ or P_{m-1}, then $|B| = |G : A| = \prod_{i=1}^{m-1}(q^i + 1)$ and (9) gives $N_G(\Omega_{2m-1}(q)) = B\,P_{m-1}$. Hence by [33], one of the following holds:

(1) $B \leq N_G(\Omega_{2m-2}^-(q))$

(2) $m = 4, q = 3$ and B lies in the normalizer of S_9, $Sp_6(2)$ or $2^6.A_7$.

In case (1) we get a factorization $N_G(\Omega_{2m-2}^-(q)) = B\,P_{m-2}$, which forces $m = 4, q = 3$ and $B \leq N_G(L_3(4))$ (the $L_3(4)$ lying in a subgroup N_2^- of L). But $N_G(L_3(4))$ has no subgroup of order $(3+1)(3^2+1)(3^3+1)$ (see for example [9]). Likewise, neither do the normalizers of S_9, $Sp_6(2)$ or $2^6.A_7$, so case (2) is also out.

Next consider $A = N(SL_m^\epsilon(q))$. Then

$$|B| = \frac{1}{t} q^{m(m-1)/2} \prod_{i=1}^{m-1} (q^i + \epsilon^i),$$

where $t \leq 4$. Now (9) gives a factorization of type $O_{2m-1}(q) = BN(SL_{m-1}^\epsilon(q)) \leq BN_1^\epsilon$. By [33], the only maximal factorizations of $O_{2m-1}(q)$ with one factor N_1^ϵ and the second divisible by $|B|$ have the second factor equal to $N_1^{-\epsilon}$, with $q = 2$ or 4. This leads to a factorization of type $N(O_{2m-2}^{-\epsilon}(q)) = BN_1$. However, Lemma 4.4 implies that there is no factorization of $O_{2m-2}^{-\epsilon}(q)$ with one factor N_1 and the other divisible by $|B|$. This forces $B \geq \Omega_{2m-2}^{-\epsilon}(q)$, but this contradicts the formulae given above for $|B|$.

Now suppose that $A = N_G(PSp_2(q) \otimes PSp_m(q))$ (m even, $q > 2$). Here $|B|_{p'} = (\prod_{i=0}^{\frac{m}{2}-2}(q^{m+2i} - 1))/(q^2 - 1)$, and (9) gives rise to a factorization of type $O_{2m-1}(q) = BN(PSp_2(q) \otimes PSp_{m-2}(q)) \leq BN_1^+$. However, [33] shows that there is no such factorization with the given value of $|B|_{p'}$.

Next let $A = N_G(\Omega_m^+(q^2))$ (m even, $q = 2,4$). Here $|B| = \frac{1}{4}q^{m^2/2}(q^{2m-2} - 1)(q^{2m-6}-1)\cdots(q^2-1)$, and (9) gives a factorization of type $Sp_{2m-2}(q) = BO_{m-1}^+(q^2) < BP_1$. Clearly $B \not\geq Sp_{2m-2}(q)$, so from [33] we see that either $B \leq N(Sp_{2a}(q^b))$ ($ab = m-1$, $b > 1$) or $B \leq N(G_2(q))$ ($m = 4$). The first case is impossible since $|N(Sp_{2a}(q^b))|$ is not divisible by the above expression for $|B|$. In the second case we must have $B \geq G_2(q)'$, and now we see as in the case (3ii) of (10.3) above, that A and $G_2(q)$ both contain conjugates of an element of order $q+1$, which contradicts the exact factorization $G = AB$.

To complete this case (11.2), assume now that $A = N_G(\Omega_8^-(q^{1/2}))$ ($m = 4$, q square). Then $|B| = q^6(q+1)(q^3+1)(q^4-1)$ and $A \cap N_1 \triangleleft G_2(q^{1/2})$, so (9) gives a factorization of type $O_7(q) = BG_2(q^{1/2}) < BG_2(q)$. Hence [33] implies that $B \leq N(\Omega_6^-(q))$. However $|\Omega_6^-(q)| = |B| \cdot (q-1)$ and $q > 2$ (since q is square), so this is impossible.

Case (11.3) Here $|B| = \frac{1}{2}q^{2m-2}(q^m-1)(q^{m-1}-1)/(q+1)$. If $B \leq P$ with $P = P_m$ or P_{m-1}, the stabilizer of a totally singular m-space W, then $A \cap B$ fixes an $(m-2)$-subspace of W, so writing $\bar{B} = BQ/Q$ we get a factorization of type $GL_m(q) = \bar{B}P_{m-2}$. By [33] this forces either $\bar{B} \geq SL_m(q)$ or $m = 5, q = 2$ and $\bar{B} \leq \Gamma L_1(2^5)$, both of which possibilities conflict with the above formula for $|B|$. Similarly if $B \leq N_G(SL_m(q))$ we get a factorization $N_G(SL_m(q)) = BN_{2,m-2}$, which forces $B \geq SL_m(q)$, a contradiction.

Case (11.4) Here $|B| = (q^m-1)(q^{m-1}+1)/(q-1)$ and we have a factorization $N_G(SU_m(q)) = BP_1$, which by [33] forces $m = 4, q = 3$ and $B \leq N(L_3(4))$. But $N(L_3(4))$ has no subgroup of order $28 \cdot 40$, a contradiction.

Case (11.5) Here $|B| = \frac{1}{t}q^{m(m-1)/2}\prod_{i=1}^{m-1}(q^i + (-1)^i)$ with $t \leq 4$, and writing $\bar{B} = BQ/Q$ (where Q is the unipotent radical of P_1), we have a factorization of type $O_{2m-2}^+(q) = \bar{B}P_1$. This forces $\bar{B} \geq \Omega_{2m-2}^+(q)$ by [33], which is impossible.

Case (11.6) Here $|B| = \frac{1}{2}q^{2m-2}(q^m-1)(q^{m-1}+1)/(q-1)$ and we have a factorization $N_G(SU_m(q)) = BN_2$, giving a contradiction using [33].

Case (11.7) Here $|B|$ is as in (11.5) and the factorization $N_2^+ = B(A \cap N_2^+)$ gives rise to a factorization of type $O_{2m-2}^+(4) = B\,N(SU_{m-2}(4)) \leq BN_2^+$. This leads to the usual contradiction using [33].

Case (11.8) Here $L = P\Omega_{16}^+(q)$, $A = N_G(\Omega_9(q))$ and $B \leq N_1$. From [33, Appendix 3] we see that $A \cap N_1 \triangleright \Omega_7(q)$, fixing a non-degenerate 8-dimensional subspace of the underlying 16-dimensional orthogonal space for G. Thus (9) gives rise to a factorization of type $O_{15}(q) = BN_8$. However there is no such factorization unless $B \geq \Omega_{15}(q)$, which is a contradiction.

Case (11.9) Here $A \cap N_1 = Co_3$ by [33, Lemma B, p.79], so (9) gives a factorization $Sp_{22}(2) = BCo_3$. However there is no such factorization with B proper in $Sp_{22}(2)$, a contradiction.

Case (11.10) Consider first $L = \Omega_8^+(2)$. Then, adjusting A, B by a triality automorphism of L if necessary, and noting that the case $A = N_1$ has been done in Section 9, we may assume that one of the following holds:

(a) $A = A_9$, $B \leq N_1, P_1$ or N_2^-;
(b) $A = P_1$ or N_2^-, $B \leq A_9$;
(c) $A = A_5^2.2^2$, $B \leq N_1$.

Consider (a). If $B \leq N_1$ then since $A \cap N_1 = L_2(8).3$ (see [33]), we have a factorization $N_1 = Sp_6(2) = B(L_2(8).3)$. This is considered in case (2i) of (10.3), where it is shown that there is a unique possible such exact factorization with $B = 2^4.A_5$; hence we have the example

$$\Omega_8^+(2) = A_9\ (2^4.A_5)$$

in Table 16.1.

When $B \leq P_1$ (still in case (a)), apply triality to take $A = A_9$ to be embedded in $\Omega_8^+(2)$ with the natural module $V = V_8(2)$ being an irreducible constituent of the permutation module for A over $\mathbb{F}_2$, and $B \leq P_3$ or P_4 (see [9, p.85]). Write vectors of V as subsets of $\{1, \ldots, 9\}$ of even size (addition being symmetric difference), and define W to be the 4-space spanned by the vectors $1234, 1256, 1278, 1357$. Then W is totally singular and an easy check shows that $C_A(W) = 1$. We know from [33] that $L = AL_W$ and $A \cap L_W = 2^3.L_3(2)$; moreover if we write $L_W = QR$ where $Q = C_L(W) = 2^6$ is the unipotent radical, and $R \cong L_4(2)$ a Levi subgroup, then $A \cap Q = 1$. Hence (9) gives a factorization $L_W = B(A \cap L_W)$, which forces B to be of the form $Q.F$, where $F \leq R$ is a group of order 15 such that $R = L_4(2) = (2^3.L_3(2))F$. Hence we have the example

$$\Omega_8^+(2) = A_9\ (2^6.15)$$

in Table 16.1.

To complete case (a), suppose $B \le N_2^-$. Note that $|B| = |L : A| = 2^6{\cdot}3{\cdot}5$ and $N_2^- = (3 \times U_4(2)).2$. It follows using [9, p.26] that $B \le (3 \times 2^4.A_5).2$ with index 6, and hence that $B = 2^4.A_5$ or $(3 \times 2^4.D_{10}).2$. The first case has been handled above, so assume $B = (3 \times 2^4.D_{10}).2$. By the $2^4.A_5$ case above, the subgroup $3 \times 2^4.D_{10}$ is semiregular on L/A with 2 orbits. The normalizer of the D_{10} in $A_5.2 = S_5$ is 5.4, and hence there are no involutions in $B \backslash (3 \times 2^4.D_{10})$. It follows that B is regular on L/A, giving the example

$$\Omega_8^+(2) = A_9\ (3 \times 2^4.D_{10}).2$$

in Table 16.1.

Now consider case (b). If $A = P_1$, then $|B| = 135$ and $A \cap A_9 = 2^3.L_3(2)$. But A_9 has no exact factorization of the form $B(2^3.L_3(2))$. And if $A = N_2^-$, then $|B| = 1120$ and $A \cap A_9 = 3^3.S_3$, but there is no exact factorization $A_9 = B(3^3S_3)$, a contradiction.

Finally consider (c): $A = A_5^2.2^2$, $B \le N_1$. Here $B \le Sp_6(2)$ and $|B| = 12096$, which forces $B = G_2(2)$, giving a possible exact factorization $\Omega_8^+(2) = (\Omega_4^+(4).2^2)G_2(2)$. However the two factors in fact share an element of order 3, as in (3ii) of (10.3), which gives a contradiction.

This completes the analysis for $L = \Omega_8^+(2)$.

Now suppose that $L = P\Omega_8^+(3)$. Again adjusting A, B by a triality automorphism of L if necessary, and noting that the case $A = N_1$ has been handled in Section 9, we may assume that one of the following holds:

(a) $A = N_G(\Omega_8^+(2))$, $B \le N_1, P_1$ or P_{13};
(b) $A = P_1$ or P_{13}, $B \le N_G(\Omega_8^+(2))$;
(c) $A = N(2^6.A_8)$, $B \le P_1$;
(d) $A = P_1$, $B \le N(2^6.A_8)$.

Consider case (a). Here $|B| = |G : A| = 3^7 \cdot 13$. Suppose $B \le P_1 = QR$, where $Q = 3^6$ and $R = L_4(3).[2^a]$ $(a \le 3)$. From [33, p.107] we have $A \cap P_1 \cap L = (3 \times PSp_4(3)).2$, and hence, writing bars for images modulo Q, we have a factorization of type $L_4(3) = \bar{B}\, PSp_4(3)$. It follows that $B \cap Q = 3^3$ and $B = 3^3.(3^3.13.3)$. However a computation using Magma [6], kindly carried out for us by Michael Giudici, showed that no such regular subgroups exist for this action.

If $B \le P_{13}$ then as B has odd order it also lies in P_1, a case already considered. And if $B \le N_1$ then by [33] we have $A \cap N_1 \cap L = 2^6.A_7$, giving a factorization of type $O_7(3) = B\,(2^6.A_7)$. Hence from [33] we see that B

lies in a parabolic subgroup of N_1, hence in a parabolic of G, which we have already excluded.

Now consider (b). If $A = P_{13}$ then $|B| = 2^8 \cdot 5 \cdot 7$; however $O_8^+(2)$ has no subgroup of this order, so this is impossible. Now assume that $A = P_1$. Then $|B| = 1120$ and $A \cap \Omega_8^+(2) = (3 \times U_4(2)).2$. Hence the factorization $N_G(\Omega_8^+(2)) = B\,(A \cap N_G(\Omega_8^+(2))$ implies that B lies in the normalizer of either $Sp_6(2)$ or A_9. The latter is impossible as neither A_9 nor S_9 has a subgroup of order 1120. The former case gives a factorization of type $Sp_6(2) = B\,N(SU_3(2)) \leq B\,O_6^-(2)$. Hence, using [33] and the fact that $|B| = 1120$, we see that $B \leq N(\Omega_6^+(2)) = N(A_8)$. However this does not have a subgroup of order 1120.

In case (c), we have $|B| = 3^{10}{\cdot}5{\cdot}13$; but the Levi factor $L_4(3)$ of P_1 has no subgroup of odd order divisible by $5 \cdot 13$; similarly, in case (d), $|B| = 2^5 \cdot 5 \cdot 7$, but $N(2^6.A_8)$ has no subgroup of this order.

This completes the analysis for $L = P\Omega_8^+(3)$.

Finally, note that for $L = \Omega_8^+(4)$, the factorizations given at the bottom of [33, Table 4] have already been considered in versions adjusted by triality, under (11.2) and (11.3).

The proof of Theorem 1.1 for classical groups is now complete.

12 Proof of Theorem 1.1: exceptional groups of Lie type

In this rather brief section, we note that when L is an exceptional group of Lie type, all (maximal or non-maximal) factorizations of L and its automorphism groups are given in [33, Table 5] (taken from [19]), and it is clear from the short list of factorizations in this table that none of them is exact. Theorem 1.1 for exceptional groups follows immediately.

13 Proof of Theorem 1.1: alternating groups

A complete description of the exact factorizations of the alternating and symmetric groups appears in the paper of Wiegold and Williamson [43]. We analyze their results to obtain our Table 16.2. An alternative starting point would be [33, Theorem D and Remark 2], which gives all the maximal factorizations. We postpone dealing with the automorphisms of A_6 outside S_6 till the end of this section.

Thus G is A_m or S_m, acting naturally on the set Ω of size $m \geq 5$. Assume that $G = AB$ with A a maximal subgroup and B regular on the set of cosets of A in G. The general case to consider is where for some k with $1 \leq k \leq 5$, one of A and B normalizes a subgroup A_{m-k} of G acting naturally on a subset Γ of Ω of size $m - k$, and the other is k-homogeneous on Ω. (In fact, this is so unless m is 6 or 8, cases considered later.)

Assume first that A_{m-k} is normal in A. By maximality of A, it follows that $A = G \cap (S_{m-k} \times S_k)$. Then B is sharply k-homogeneous on Ω. If $k = 1$, we get the standard examples $S_n = S_{n-1}\ B$ with B regular on Ω, and similarly for A_n. For $k > 1$ we use Kantor's list [23]; the possibilities are listed in [43]. For $k = 2$, we see that B must have odd order and it follows that $m = q$ is a prime power congruent to 3 mod 4 and B is a subgroup of $AGL_1(q)$ of order $q\frac{q-1}{2}$, yielding the example

$$A_q = S_{q-2}\ ([q]\frac{q-1}{2})$$

in Table 16.2. For $k = 3$ we get the two examples with

$$A_{32} = (A_{29} \times A_3).2\ (A\Gamma L_1(32)),$$

$$A_8 = (A_5 \times A_3).2\ (AGL_1(8)).$$

There are no sharply k-homogeneous examples with $k = 4$ and $k = 5$.

Assume next that A is the k-homogeneous factor, which now must be maximal in G. We consider the various cases in the Theorems in [43]. In Theorem A there, G is alternating, and in Theorem S it is symmetric.

In case (AI) (of [43]), we have G alternating, A is sharply k-transitive and $B = A_{m-k}$. The possibilities are well known and are listed in [43, Remarks, p.173]. Certainly $k > 1$ by maximality of A. Next, $k > 2$, since there are no maximal sharply 2-transitive groups in A_m. If $k = 3$ we have A a Zassenhaus group; since A is sharply 3-transitive and maximal in A_m, we get $A = PSL_2(p^2).2$ with p a prime congruent to 3 mod 4. This gives examples in Table 16.2:

$$A_{p^2+1} = PSL_2(p^2).2\ (A_{p^2-2}).$$

If k is 4 or 5, the only sharply k-transitive groups are the Mathieu groups M_{11} and M_{12}, and we get the examples

$$A_m = M_m\ A_7\ \ (m = 11, 12).$$

In case (AII), G is alternating and A is k-homogeneous but not k-transitive on Ω. The possibilities are listed in [43, p.173]. Those leading to maximal subgroups of G lead to the factorizations

$$A_9 = (L_2(8).3)\ S_5,$$

$$A_{33} = (L_2(32).5)\ (A_{29} \times A_3).2,$$

$$A_p = (p.\frac{p-1}{2})\ S_{p-2} \text{ with } p \text{ prime, } \ p \equiv 3 \bmod 4, \ p \neq 7, 11, 23,$$

$$A_{p+1} = L_2(p)\ S_{p-2} \text{ with } p \text{ prime, } \ p \equiv 3 \bmod 4, \ p \neq 7, 11, 23.$$

Note that in the last two lines the congruence on p is needed to obtain a factorization (see [43, Theorem A]); for $p \equiv 1 \bmod 4$, we shall meet the corresponding factorizations for the symmetric groups below, which explains why they appear in Table 16.2 with a *. The excluded values are there to rule out non-maximal cases – they do occur below for the relevant symmetric groups and hence appear in Table 16.2 with a †.

Next we consider the cases in Theorem S, where G is symmetric. In case (SIi), we have precisely the trivial factorization $S_m = A_m\ 2$, which is ruled out by our conditions. In case (SIii), the maximal subgroup A contains $A \cap A_m$ as a subgroup of index 2 which is sharply k-transitive on Ω, There is no such maximal subgroup with $k = 1$: it would have to be primitive on Ω, so would have to be dihedral of order $2p$, but that is not maximal either. Further, there is no such maximal subgroup with $k = 2$: A would have to be soluble, so $A = AGL_1(p)$ - but then the intersection with the alternating group is no longer 2-transitive on Ω. Thus $k = 3$ and A is maximal and contains a sharply 3-transitive subgroup of index 2; we deduce that $A = P\Gamma L_2(p^2)$ with p congruent to 3 mod 4, and we have seen the correponding factorizations of the alternating groups above in case (AI). In cases (SIiii) and SIIi), we have A sharply k-transitive on Ω. If $k = 4$ or $k = 5$, there is no such maximal sharply k-transitive subgroup, and also $k > 1$ by maximality. For $k = 2$, we have $A = AGL_1(p)$ with p a prime, and we get the exact factorizations

$$S_p = AGL_1(p)\ S_{p-2}$$

and

$$S_p = AGL_1(p)\ (A_{p-2} \times 2) \ \ (p \equiv 1 \bmod 4).$$

For $k = 3$, we have $A = PGL_2(p)$ with p a prime (for maximality), and we get the factorizations

$$S_{p+1} = PGL_2(p)\ S_{p-2}$$

and

$$S_{p+1} = PGL_2(p)\ (A_{p-2} \times 2)\ \ (p \equiv 1 \bmod 4).$$

These are listed in Table 16.2, with appropriate remarks. In case (SIIii), A is k-homogeneous but not k-transitive on Ω. The possibilities are listed in [43, p.176]. None of these is maximal in S_m.

Next we consider the cases where m is 6 or 8 and neither A nor B normalizes a large natural alternating subgroup – see cases (AIII) and (SIII) of [43]. We obtain the exact factorizations

$$S_6 = L_2(5).2\ B \ \text{ with } B \text{ either } C_6 \text{ or } D_6,$$

$$A_8 = AGL_3(2)\ C_{15}.$$

Finally, to complete the treatment of groups with alternating socle, we consider the case $m = 6$ where G contains an automorphism of A_6 not contained in S_6. By [9], maximal subgroups of G have intersection with A_6 of order $10, 36$ or 8, so the index is $36, 10$ or 45, respectively. There is no subgroup of order 45, so the last is out. If $A \cap A_6 = D_{10}$, since there is only one class of involutions in A_6 and since the factorization is exact, we must have $B \cap A_6 = 3^2$ and $G = A_6.2^2$. Thus $B = 3^2 2^2$. On the other hand, the extension $A_6.2_3$ is non-split, so this cannot work. Finally, in the remaining case $A = N(3^2)$, there are factorizations both with $B = C_{10}$ and $B = D_{10}$ in $G = A_6.2_2 = PGL_2(9)$: here $B < D_{20}$; the cyclic group C_{10} (the Singer cycle in $PGL_2(5)$) is clearly transitive in the action of degree 10, and since D_{20} is isomorphic to $D_{10} \times C_2$, there is also a dihedral subgroup D_{10} which is transitive.

This completes the consideration of groups with alternating socles.

14 Proof of Theorem 1: sporadic groups

We argue separately for each of twelve sporadic simple groups (and their automorphism groups) which have a factorization. By [33], these are the five Mathieu groups, $J_2, HS, He, Ru, Suz, Fi_{22}$ and Co_1. Suppose that $G = AB$, $A \cap B = 1$ and A max G. We aim to show that this exact factorization is in Table 16.3, and that all such factorizations exist.

Case M_{11}: Since M_{11} has a unique conjugacy class of involutions, either A or B has odd index in L. From the list of factorizations in [33], we see that B cannot have odd index. Hence $|L : A|$ is odd. If $A = M_{10}$, we get

$$M_{11} = M_{10}\ 11$$

as the only possibility. If $A = M_9.2$, we get

$$M_{11} = (M_9.2)\ (11.5)$$

as the only possibility. And if $A = 2S_4$, there are no possibilities for B.

Case M_{12}**:** First consider the factorization $M_{12} = M_{11}A_5$ coming from Lemma 2.6. Here the intersection of the factors has order 5. Taking a subgroup of index 5 in A_5, we get the exact factorization

$$M_{12} = M_{11}\ A_4.$$

This is the only factorization arising here: for if $A = M_{11}$ then $G = M_{12}$, since M_{11} is not maximal in $M_{12}.2$; and B is not in M_{11} since that has no subgroup of index 5.

Now we consider the factorizations arising in [33]. If $A = M_{11}$, we get exact factorizations for various subgroups B of order 12; we already noted the factorization with $B = A_4$, but others exist: a regular $B = D_{12}$ can be seen as a subgroup of $L_2(11)$, and a regular $B = 2^2 \times 3$ can be seen as a subgroup of $A_4 \times S_3$. Next let $A = L_2(11)$. Since $M_{12} = L_2(11)\ M_{11}$ with intersection of factors being 11.5 and since $M_{11} = (11.5)\, M_9.2$ is an exact factorization, we get the exact factorization

$$M_{12} = L_2(11)\ (M_9.2),$$

given in Table 16.3.

Now A cannot be $M_{10}.2$ or $M_9.S_3$, since it is easy to see that M_{12} has no subgroups of order 66 or 220. And A cannot be one of $2 \times S_5, 4^2.D_{12}, A_4 \times S_3$: here B would be a subgroup of M_{11} of index $20, 16, 6$, which is impossible.

Case M_{22}**:** The only maximal factorization to consider here (containing $G = AB$) is $M_{22}.2 = (L_2(11).2)\ (L_3(4).2)$. Now A cannot be $L_2(11).2$ since the index of this in $M_{22}.2$ is 672 and $L_3(4).2$ has no subgroup of order 672 ([9, p. 23]). On the other hand, if $A = L_3(4).2 = M_{21}.2$, we get

$$M_{22}.2 = (M_{21}.2)\ D_{22}$$

as the only possibility. This is an exact factorization: for by [9], the involution in the normaliser of an 11-subgroup is in class $2C$, being a power of an element of order 10, and these involutions are fixed point free in the natural action of degree 22. On the other hand, $M_{22}.2$ has no cyclic subgroup of order 22, so there is no other possibility for an exact factorization here.

Case M_{23}: This is very similar to the case M_{11}. Since M_{23} has a unique conjugacy class of involutions, A has odd index or odd order. If A has odd order, then $A = 23.11$. Now $B < M_{22}$ is not possible, since M_{22} has no subgroup of index 11. Hence we get precisely the two exact factorizations

$$M_{23} = (23.11)\ (L_3(4).2)$$

and

$$M_{23} = (23.11)\ (2^4 A_7),$$

as in Table 16.3. Assume now that the index of A is odd. If $A = M_{22}$, the only possibility is

$$M_{23} = M_{22}\ 23.$$

If A is $L_3(4).2$ or 2^4A_7, we get the first two examples with A and B swapped. Finally, the maximal subgroup of index 1771 does not appear as a factor in a factorization.

Case M_{24}: First let $A = M_{23}$. There are subgroups of order 24 regular here. For example, considering the factorization $M_{24} = M_{23}\ L_2(23)$ we see that

$$M_{24} = M_{23}\ D_{24}$$

is an exact factorization. And, considering the factorization $M_{24} = M_{23}\ L_2(7)$, we see that

$$M_{24} = M_{23}\ S_4$$

is an exact factorization. Next let $A = L_2(23)$. Then B is a subgroup of one of $M_{23}, M_{22}.2, 2^4A_8, L_3(4).2$ of index $253, 22, 8, 1$, respectively. Thus we get precisely the exact factorizations

$$M_{24} = L_2(23)\ (L_3(4).2)$$

and

$$M_{24} = L_2(23)\ (2^4A_7),$$

as in Table 16.3. Next, if A is $M_{22}.2, 2^4A_8$ or $L_3(4).S_3$, then B is a subgroup of $L_2(23)$ of index 22, 8 or 3, which is impossible. Finally, if A is $M_{12}.2, 2^63S_6$ or $2^6(L_3(2) \times S_3)$ then B is a subgroup of M_{23}. But B has order divisible by 23, forcing $B = 23.11$, which is not so.

Case J_2: First consider the factorization of J_2 with factors $U_3(3)$ and $A_5 \times D_{10}$. The intersection of the factors has order 6. Since $U_3(3)$ has no subgroup of index 6, we must have $A = U_3(3)$ of index 100 and B contained in the normalizer of a Sylow 5-subgroup. This does not lead to a factorization of the simple group by [33, p. 119] . Thus we are searching for subgroups B of $J_2.2$ which are regular in the action of degree 100. We claim that there is a subgroup $B = 5^2.4$ acting regularly: The argument in [33, p. 119] implies that the elements of order 4 which lie in $U_3(3).2$ are of type $4B$ whereas those normalizing a Sylow 5-subgroup are of type $4C$. Since the elements of type $4C$ square to involutions $2B$ which are not represented in $U_3(3).2$, the assertion follows. It is also not hard to see that no subgroup $B = 5^2.2^2$ would do.

Case HS: The factorizations to consider here all have one of the factors intersecting L in M_{22}, whereas the other intersects L in $U_3(5).2, (5:4) \times A_5$ or $[5^3 2^5]$. There is only one exact factorization of an automorphism group of M_{22}; it is quite easy to see that this forces A to normalize M_{22} and B to be regular of degree 100. Also, B must normalize a 5-subgroup. Looking at the permutation character of degree 100, all involutions in B must be of type $2B$. If B were contained in a subgroup $U_3(5).2$, then $B \cap U_3(5)$ would have even order. However all involutions in $U_3(5)$ are conjugate and are of type $2A$, so this is not possible.

Suppose that B contains no elements of order 4. Then, since the only involutions in B are of type $2B$, it follows that $B \subset HS$. Now the maximal subgroup $[5^3 2^5]$ of $HS \cdot 2$ meets HS in the intersection of two maximal subgroups $U_3(5).2$, so if B were contained in a subgroup $[5^3 2^5]$, then B would contain an involution from some $U_3(5)$, which is not the case. Thus $B < (5:4) \times A_5$, and in fact B lies in the normaliser $(5:4) \times (5:2)$ of a 5^2 in this subgroup. Hence B contains a conjugate of every involution in $(5:4) \times (5:2)$. However this group contains an element of type $4A$ that squares to an element of type $2A$, which is a contradiction.

Thus B contains elements of order 4. Now the only fixed point free elements of order 4 are of type $4A$ or $4F$, but the square of an element of type $4A$ has type $2A$. Thus all elements of order 4 in B must have type $4F$, and in particular $G = HS.2$ (hence the * symbol in Table 16.3). We claim that there is a subgroup of order 100 in $HS.2$ acting regularly. Consider the factorization $HS = M_{22}\ 5.4 \times A_5$. mentioned above. The second factor contains a normal subgroup P of order 5 with non-trivial elements of type $5B$. The normalizer of P in $HS.2$ is $5.4 \times S_5$. Let Q be a Sylow 5-subgroup of the S_5, and let x be an element of order 20 centralizing P and normalizing Q. This must then be an element of type $20C$, as it must square to an element of type $10B$. It follows that all non-trivial powers of x are fixed-point-free, and the group of order 100 generated by P, Q, x is the regular subgroup we want.

Case He**:** The maximal factorizations here have one factor intersecting L in $Sp_4(4).2$ and the other either in $7^2SL_2(7)$ or $7^{1+2}(S_3 \times 3)$. Since the intersection of the factors is smaller than the index of the largest proper subgroup of $Sp_4(4).4$, it follows that A must be the normalizer of $Sp_4(4)$ and B is regular of order $2058 = 7^3 6$. It follows that B lies in the normalizer of a Sylow 7-subgroup. By [33, p. 120] , it follows that $G = He.2$ (hence the * symbol in the Table). We claim that $He.2$ does have a subgroup B of order 2058 which is regular. It will suffice to show that an element of type $6E$ normalizes a Sylow 7-subgroup: for, its non-trivial powers are all fixed-point-free, as are also all the 7-elements, as we see from the permutation character in [9, p. 104]. We refer to [33, p. 120]. The centre C of a Sylow 7-subgroup P is a subgroup of order 7 with all 7-elements of type $7C$. We consider C as subgroup of the maximal subgroup $3S_7 \times 2$; there we see an element of type $3B$ acting on C and an element of type $2C$ centralizing $3S_7$, yielding an element of type $6E$ normalizing C and hence P, as required.

Case Ru**:** The only maximal factorization has factors ${}^2F_4(2)$ and $L_2(29)$, intersecting in a group of order 3. Hence there are no exact factorizations.

Case Suz**:** The maximal factorizations of Suz here have one factor $G_2(4)$ and the other either $U_5(2)$ or 3^5M_{11}, of indices $1782, 32760$ and 232960, and similarly for $Suz.2$. Sylow theory shows that Suz and $Suz.2$ have no subgroup of order $1782 = 2.3^4.11$, so $A \cap L$ is not $G_2(4)$. On the other hand, $G_2(4)$ has no exact factorizations.

Case Fi_{22}**:** The maximal factorization to consider in this case is $Fi_{22} = 2U_6(2)\,{}^2F_4(2)'$ and the corresponding factorization of $Fi_{22}.2$. Now $A \cap L$ is not $2U_6(2)$, since ${}^2F_4(2)$ and ${}^2F_4(2)'$ have no proper factorizations. If $A \cap L = {}^2F_4(2)'$, then B has order $2^6 3^6 77$. We see from [9, p. 115] that there is no suitable subgroup in $U_6(2)$.

Case Co_1**:** In the maximal factorizations here, one of the factors is a smaller Conway group while the other is the normalizer of one of $3.Suz$ or $A_4 \times G_2(4)$. Since the smaller Conway groups have no proper factorizations, it follows that A is a smaller Conway group, of index either $2^3.3^3.5.7.13$ or $2^{11}.3^2.5.7.13$. Inside $3.Suz.2$, the only maximal subgroup of order divisible by either is $G_2(4)$. On the other hand, $G_2(4)$ has no subgroups of suitable orders - see [9, p. 97].

15 Proof of Theorem 1.4 and Corollary 1.3

Most of this section is concerned with proving Theorem 1.4. At the end can be found the very short proof of Corollary 1.3.

For the proof of Theorem 1.4, we make the following assumptions.

(1) $B < G \leq S_n$ with G primitive, and B regular on Ω, where $|\Omega| = n$;

(2) $T \leq B \leq \mathrm{Aut}(T)$, where T is a nonabelian simple group;

(3) N is a minimal normal subgroup of G, with $N = U_1 \times \ldots \times U_k \cong U^k$, where U is simple and $k \geq 1$; and $\pi_i : N \to U_i$ is the natural projection map, for $i = 1, \ldots, k$.

First we reduce to the case where $T \leq N$. We shall use the fact that $|\mathrm{Out}(T)| < |T|$, and we note that this implies that $n = |B| < |T|^2$.

Lemma 15.1 *The simple group U is nonabelian, and either*

(i) $G \leq D(2,T)$, with $\mathrm{soc}(G) \cong T^2$ and $B = T \cong U$; or

(ii) $T \leq N$, and N is the unique minimal normal subgroup of G.

Proof Since B is regular, $|T|$ divides n, and in particular n is not a prime power, so N is not elementary abelian. Thus U is a nonabelian simple group, and so G permutes $\{U_1, \ldots, U_k\}$ transitively by conjugation. Since G is primitive, its normal subgroup N is transitive, so $G = NG_\alpha$, where $\alpha \in \Omega$, and G_α is also transitive on $\{U_1, \ldots, U_k\}$.

Suppose first that T centralises N. Then $C_G(N)$ is a nontrivial normal subgroup of the primitive group G, and by the O'Nan–Scott Theorem [11, Chapter 4] it follows that $C_G(N)$ and N are both regular on Ω, are isomorphic to each other, and $G \leq D(2,U) \wr S_k$ with $k \geq 1$. Thus we have $T \leq C_G(N) \cong N \cong U^k$. Since both T and U are simple, we have $|T| \leq |U|$. On the other hand, by the observation made before the proof, $|C_G(N)| = |U|^k = n < |T|^2$. It follows that $k = 1$, and so $G \leq D(2,U)$. If $T = C_G(N)$, then T is regular on Ω, and so $B = T \cong U$ and part (i) holds. So suppose that T is a proper subgroup of $C_G(N)$. Now N is the centraliser in G of $C_G(N)$, and so $B \cap N = 1$ and B is isomorphic to a subgroup of $G/N \leq \mathrm{Aut}(U)$. That is to say, we have a simple proper subgroup T of a nonabelian simple group U such that $M := N_{\mathrm{Aut}(U)}(T)$ has order divisible by $|B| = |U|$. Now $|M|$ divides $|\mathrm{Out}(U)| \cdot |M \cap U|$, and $M \cap U$ is a proper subgroup of U, so $|U : M \cap U|$ divides $|\mathrm{Out}(U)|$. However this does not hold for any nonabelian simple group U and proper subgroup $M \cap U$ (see for example [25, 5.2.2]).

Thus we may assume that T does not centralise N, and therefore $B \cap C_G(N) = 1$. Suppose that $T \not\leq N$. Then, since B is almost simple, $B \cap N = 1$ and B is isomorphic to a subgroup of $\mathrm{Out}(N) = \mathrm{Out}(U) \wr S_k$. Since $\mathrm{Out}(U)$ is soluble, it follows that B is isomorphic to a subgroup of S_k. Thus n divides $k!$. Let $\alpha \in \Omega$ and $H := N_\alpha$. As we noted above, G_α is transitive by conjugation on $\{U_1, \ldots, U_k\}$, and since G_α normalises H it follows that G_α permutes the projections $\pi_i(H)$ $(1 \leq i \leq k)$ transitively. If the $\pi_i(H) = U_i$, then $H \cong U^\ell$ for some proper divisor ℓ of k, and so $n = |N : H| = |U|^{k-\ell}$ and $k - \ell \geq k/2$. It follows that, for any odd prime divisor p of $|U|$, $p^{k-\ell}$ divides n, and hence divides $k!$. However the largest exponent of p that divides $k!$ is $[(k-1)/(p-1)] < k/2$. Thus the projections $\pi_i(H)$ are all isomorphic to a proper subgroup R of U, and by the O'Nan–Scott Theorem [11, Chapter 4], $H \cong R^k$ and $n = m^k$ where $m = |U : R|$. In this case we deduce that p^k divides $k!$ for any prime p dividing m, and we have a contradiction as in the previous case. Thus $T \leq N$.

Suppose now that G has a second minimal normal subgroup M distinct from N. Then $T \leq C_G(M)$, and the argument of the first part of the proof, with N and M interchanged, shows that part (i) holds. Finally, if N is the unique minimal normal subgroup of G then part (ii) holds. ∎

By Lemma 15.1, U is a nonabelian simple group and so G acts transitively by conjugation on $\{U_1, \ldots, U_k\}$. Let $\pi : G \to S_k$ be the homomorphism corresponding to this action.

Lemma 15.2 *One of the following holds.*

(i) $G \leq D(2, T)$, *with* $\mathrm{soc}(G) = T^2$ *and* $B = T \cong U$*;*

(ii) $G \leq H \wr S_k$ *in product action, where* $U \leq H \leq \mathrm{Aut}(U)$*,* $k \geq 2$*,* $\pi(B) \neq 1$*, and* $B \neq T$*;*

(iii) $k = 1$.

Proof Suppose that neither case (i) nor case (iii) holds. Then $k \geq 2$ and, by Lemma 15.1, $T \leq N \cong U^k$ so that $|T| \leq |U|$, and N is the unique minimal normal subgroup of G. Also, as we observed above, $|T| > n^{1/2}$. If $n = |U|^\ell$ for some integer $\ell \geq k/2$, then we have $|U| \geq |T| > |U|^{\ell/2}$ which implies that $\ell = 1$ and $k = 2$. By the O'Nan–Scott Theorem, we have in this case that $G \leq D(2, U)$. The argument in the second paragraph of the proof of Lemma 15.1 yields that part (i) holds, contrary to our assumptions. Thus n is not of this form.

Let $\alpha \in \Omega$. It now follows from the O'Nan–Scott Theorem that $N_\alpha = R_1 \times \ldots \times R_k = R^k$ with $R_i < U_i$ and $R_i \cong R$, a proper subgroup of U, and $G \leq H \wr S_k \leq S_m \wr S_k$ in product action on $\Omega = \Omega_0^k$, where $m = |\Omega_0| = |U : R|$ and $U \leq H \leq \mathrm{Aut}(U)$. Let $M = G \cap S_m^k$, and note that $N \leq M$.

Next we show that $\pi(B) \neq 1$. Suppose that this is not so. Then $B \leq M$. Let $\alpha = (\alpha_1, \ldots, \alpha_k)$, and for $i = 1, \ldots, k$, let M_i denote the setwise stabiliser in M of $\{\gamma \in \Omega | \gamma_i = \alpha_i\}$. Then $M_\alpha = \cap_{i=1}^k M_i$, and for each i, M factorizes as $M = M_i(\cap_{j \neq i} M_j)$. Since $B \leq M$ and B is transitive, we have also, setting $B_i := B \cap M_i$, the equality $|B_i| = |B|/|\Omega_0|$ and the factorization $B = B_i(\cap_{j \neq i} B_j)$ for each i. If $k \geq 3$, these factorizations are called strong multiple factorizations, and all such factorizations of finite almost simple groups B have been classified in [3]; in none of the examples are the subgroups B_i all of the same size. Thus $k = 2$. In this case we have $B = B_1 B_2$ and $B_1 \cap B_2 = B_\alpha = 1$. All factorizations of a finite almost simple group B in which the factors B_1, B_2 have the same order have also been classified in [3], and for none of them do the factors intersect in the identity subgroup. This contradiction proves that $B \not\leq M$, or equivalently, that $\pi(B) \neq 1$. In particular, since $T \leq N \leq M$, this means that $B \neq T$. ∎

Proof of Theorem 1.4.

Let T, B, G, N be as defined at the beginning of this section, and suppose first that $B = T$. If $G \leq D(2, T)$ with $\mathrm{soc}(G) = T^2$, then part (ii) of Theorem 1.4 holds. So we now assume that this is not the case. Then by Lemmas 15.1 and 15.2, it follows that G is almost simple with socle N containing T. If $N = A_n$ then $|T| = n$, and part (i) of Theorem 1.4 holds, so assume that $N \neq A_n$. Then it follows from Theorem 1.1, and inspection of Tables 16.1 to 16.3, that T, G satisfy one of the first three lines of Table 2 in part (iii) of Theorem 1.4.

Thus we may assume that $B \neq T$. Suppose first that G is almost simple. If G contains A_n then part (i) holds, so assume this is not the case. Then, by Theorem 1.1 and inspection of Tables 16.1 to 16.3, B, G are as in one of the lines of the second section of Table 2 in part (iii) of Theorem 1.4.

Assume now that $k \geq 2$. Then, by Lemma 15.2, $G \leq H \wr S_k$ in product action on $\Omega = \Omega_0^k$, where $U \leq H \leq \mathrm{Aut}(U)$, and $N_\alpha = R^k$ where $m = |\Omega_0| = |U : R|$. Further, $\pi(B) \neq 1$. Suppose that G is chosen to satisfy these conditions, with k minimal subject to $k \geq 2$. Let $\alpha = (\delta, \ldots, \delta) \in \Omega$, where $\delta \in \Omega_0$.

We claim that $\pi(B)$ is transitive. Since $\pi(B) \neq 1$, $\pi(B)$ has an orbit of length $\ell \geq 2$. Without loss of generality we may suppose that this orbit is $\{1, \ldots, \ell\}$. If $\ell < k$, then $C := \{\gamma \in \Omega | \gamma_i = \delta \text{ for } \ell < i \leq k\}$ is a block of imprimitivity for B in Ω, and the setwise stabiliser B_C is regular on C and is almost simple with socle T. Moreover, the setwise stabiliser in G of C induces on C a primitive subgroup of $H \wr S_\ell$ in product action, and the group B_C projects onto a transitive subgroup of S_ℓ. This contradicts the minimality of k, and hence we conclude that $\pi(B)$ is transitive.

We claim that there is a prime p dividing $|T|$ such that p does not divide $|B : T|$ and such that a Sylow p-subgroup of T is cyclic. This follows from [16, 4.10.3(a)] if T is of Lie type, and is clear if T is alternating or sporadic.

Let p be as in the previous paragraph, and let P be a Sylow p-subgroup of T. Write $|P| = p^a$ and let P_0 be the subgroup of P of order p. Since p does not divide $|B : T|$ it follows that $P \leq T \leq B \cap H^k$. Suppose that p^a does not divide m. Then P_0 fixes some point of Ω_0, say ω, and hence P_0 fixes the point $(\omega, \ldots, \omega) \in \Omega$. This is a contradiction since $P_0 \leq B$ and B is regular. Therefore p^a divides m and so p^{ak} divides $n = |B|$. This, however, implies that $p^{a(k-1)}$ divides $|B : T|$ which is a contradiction. This completes the proof of Theorem 1.4. ∎

Proof of Corollary 1.3

Let G be almost simple and primitive of degree n, and assume that G has a regular subgroup B. Suppose that $G < H < S_n$, where $\mathrm{soc}(G) \neq \mathrm{soc}(H)$ and $\mathrm{soc}(H) \neq A_n$. If H is almost simple then it follows from Theorem 1.1 that (iii) holds. So suppose that H is not almost simple. Then, by [40, Proposition 6.1], either $G = PSL_2(7)$, $H = AGL_3(2)$ of degree 8, or $\mathrm{soc}(G) = A_6$, M_{12} or $PSp_4(q)$ (with q even), of degree m^2 and $H \leq S_m \wr S_2$, where $m = 6, 12$ or $q^2(q^2-1)/2$ respectively. The group $PSL_2(7)$ contains a regular subgroup, giving case (ii) of the corollary. However, Theorem 1.1 shows that none of the above primitive groups of degree m^2 possesses a regular subgroup (note that for $G = M_{12}.2$, $G_\alpha = L_2(11).2$, we have $G_\alpha \cap \mathrm{soc}(G)$ non-maximal in $\mathrm{soc}(G)$, so this is not the example in line 4 of Table 16.3). This completes the proof.

16 The tables in Theorem 1.1

In this section we present the tables of regular subgroups referred to in our main result, Theorem 1.1. The first two columns of each table contain the possibilities for the simple group L and a point stabilizer in L. The third has the possibilities for the regular subgroup B, and in the fourth we give the number of possibilities for B up to conjugacy in $\mathrm{Aut}\, L$. (We have not included this column in Table 16.2, where the numbers of classes are rather clear.) The last column contains any relevant extra information. This includes the use of the symbols $*$ and †, which (as in [33]) have the following meaning. *The symbol $*$ means that there is no regular subgroup B in the simple group L, but there is one in some almost simple group with socle L; and † means that $G_\alpha \cap L$ is not maximal in L, but G_α is maximal in some almost simple group G with socle L.*

Some of the numbers of classes in column 4 of Tables 16.1 and 16.3 were calculated by Michael Giudici using Magma, and more information about the sporadic group examples in Table 16.3 can be found in [15].

Table 16.1: L of Lie type

L	$G_\alpha \cap L$	B	no. of classes	Remark
$L_n(q)$	P_1 or P_{n-1}	$[\frac{q^n-1}{q-1}]$	see (5.1)	B metacyclic, $B \leq \Gamma L_1(q^n)/\mathbb{F}_q^*$
$L_2(q)$	D_{q+1}	$[\frac{q(q-1)}{2}]$	see (5.5)(β)	$q \equiv 3$ mod 4, $B \leq P_1$, $\dagger$ if $q = 7$
$L_5(2)$	P_2 or P_3	31.5	1	
	31.5	P_2 or P_3	2	
$L_2(11)$	P_1	A_4	1	
	A_5	11	1	
	A_4	11.5	1	$\dagger, G = L.2$
$L_2(23)$	P_1	S_4	1	
	S_4	$P_1 = 23.11$	1	
$L_2(29)$	A_5	29.7	1	
$L_2(59)$	P_1	A_5	1	
	A_5	$P_1 = 59.29$	1	
$L_3(3)$	13.3	$3^2.[16]$	1	
$L_3(4)$	7.3	$(2^4.(3 \times D_{10}).2$	1	$*, G \geq L.S_3$
$L_4(3)$	$(4 \times L_2(9)).2$	$3^3.\Gamma L_1(3^3)$	1	$*, G = L.2 = PGL_4(3)$
$L_4(4)$	$(5 \times L_2(16)).2$	$2^6.\Gamma L_1(2^6)$	1	$*, G = L.2$
$U_3(8)$	P_1	3×19.9	1	$*, G \geq L.3^2$
	19.3	P_1	1	$*, G \geq L.3^2$
$U_4(2)$	P_2	[27]	2	
$U_4(3)$	$L_3(4)$	$[3^4.2]$	6	$*, G \geq L.2$
$U_4(8)$	P_2	$GU_1(2^9).9$	1	$*, G \geq L.3$
$Sp_4(4)$	$L_2(16).2$	S_5	1	$*, G = L.2$
$Sp_6(2)$	$G_2(2)$	S_5	2	
	$L_2(8).3$	$2^4.A_5$	1	
$PSp_6(3)$	$L_2(27).3$	$3^{1+4}.2^{1+4}.5.4$	1	$*, G = L.2$
$Sp_6(4)$	$G_2(4)$	$L_2(16).4$	1	$*, G = L.2$
$Sp_8(2)$	$O_8^-(2)$	S_5	1	
$\Omega_8^+(2)$	$\Omega_7(2)$	S_5	1	
	A_9	$2^4.A_5$	1	
	A_9	$2^6.15$	1	
	A_9	$(3 \times 2^4.D_{10}).2$	1	
$\Omega_8^+(4)$	$\Omega_7(4)$	$L_2(16).4$	1	$*, G \geq L.2$

Table 16.2: L alternating

L	$G_\alpha \cap L$	B	Remark
A_n	A_{n-1}	any $B, \|B\| = n$	
A_q (q prime power)	S_{q-2}	$\mathbb{F}_q.\frac{q-1}{2} < AGL_1(q)$	$q \equiv 3 \bmod 4$
A_p, A_{p+1} (p prime)	$p.\frac{p-1}{2}$, $L_2(p)$(resp.)	S_{p-2}	† if $p = 7, 11, 23$
			$*$ if $p \equiv 1 \bmod 4$
		$A_{p-2} \times 2$	$*$, $p \equiv 1 \bmod 4$
A_{p^2+1} (p prime)	$L_2(p^2).2$	A_{p^2-2}	$p \equiv 3 \bmod 4$
A_6	$L_2(5)$	C_6, S_3	$*$
	$N(3^2)$	C_{10}, D_{10}	$*$, $G \not\leq S_6$
A_8	$AGL_3(2)$	C_{15}	
	$(A_5 \times A_3).2$	$AGL_1(8)$	
A_9	$L_2(8).3$	S_5	
A_{11}, A_{12}	M_{11}, M_{12} (resp.)	A_7	
A_{32}	$(A_{29} \times A_3).2$	$A\Gamma L_1(32)$	
A_{33}	$L_2(32).5$	$(A_{29} \times A_3).2$	

Table 16.3: L sporadic

L	$G_\alpha \cap L$	B	no. of classes	Remark
M_{11}	M_{10}	11	1	
	$M_9.2$	11.5	1	
M_{12}	M_{11}	[12]	3	see [15]
	$L_2(11)$	$M_9.2$	1	
M_{22}	M_{21}	D_{22}	1	$*$
M_{23}	M_{22}	23	1	
	$M_{21}.2$	23.11	1	
	23.11	$M_{21}.2$	1	
	$2^4.A_7$	23.11	1	
	23.11	$2^4.A_7$	1	
M_{24}	M_{23}	[24]	8	see [15]
	$L_2(23)$	$M_{21}.2$	1	
	$L_2(23)$	$2^4.A_7$	1	
J_2	$U_3(3)$	$5^2.4$	2	$*$, see [15]
HS	M_{22}	$5^2.4$	4	$*$, see [15]
He	$Sp_4(4).2$	$7^{1+2}.6$	3	$*$, see [15]

References

[1] H.H. Andersen, J. Jorgensen and P. Landrock, The projective indecomposable modules of $SL(2, p^n)$, *Proc. London Math. Soc.* **46** (1983), 38-52.

[2] M. Aschbacher and G.M. Seitz, Involutions in Chevalley groups over fields of even order, *Nagoya Math. J.* **63** (1976), 1–91.

[3] R.W. Baddeley and C.E. Praeger, On classifying all full factorisations and multiple-factorisations of the finite almost simple groups, *J. Algebra* **204** (1998), 129–187.

[4] B. Baumeister, Primitive permutation groups of unitary type with a regular subgroup, *Bull. Belg. Math. Soc. Simon Stevin* **12** (2005), 657–673.

[5] B. Baumeister, Primitive permutation groups with a regular subgroup, *J. Algebra* **310** (2007), 569–618.

[6] W. Bosma, J. Cannon and C. Playoust, The MAGMA algebra system I: The user language, *J. Symbolic Comput.* **24** (1997), 235–265.

[7] P.J. Cameron and W.M. Kantor, 2-transitive and antiflag transitive collineation groups of finite projective spaces, *J. Algebra* **60** (1979), 384–422.

[8] P.J. Cameron, P.M. Neumann and D.N. Teague, On the degrees of primitive permutation groups, *Math. Z.* **180** (1982), 141–149.

[9] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *Atlas of Finite Groups*, Oxford University Press, 1985.

[10] J. A. de Séguier, *Éléments de la théorie des groupes abstraits*, Gauthier-Villars, Paris, 1904.

[11] J.D. Dixon and B. Mortimer, *Permutation groups*, Springer-Verlag, Graduate Texts in Mathematics **163**, New York, 1996.

[12] P. Etingof, S. Gelaki, R.M. Guralnick amd J. Saxl, Biperfect Hopf Algebras, *J.Algebra* **232** (2000), 331–335.

[13] X.G. Fang, C.E. Praeger, and J. Wang, On the automorphism groups of Cayley graphs of finite simple groups, *J. London Math. Soc. (2)* **66** (2002), 563–578.

[14] D.A. Foulser, The flag-transitive collineation groups of the finite Desarguesian affine planes, *Canad. J. Math.* **16** (1964), 443–472.

[15] M. Giudici, Factorizations of sporadic simple groups, *J. Algebra* **304** (2006), 311–323.

[16] D. Gorenstein, R. Lyons and R. Solomon, *The classification of the finite simple groups, Volume 3*, Math. Surveys and Monographs, Vol. 40 , No. 3, American Math. Soc., 1998.

[17] P. Hegedüs, Regular subgroups of the affine group, *J. Algebra* **225** (2000), 740-742.

[18] A. Heinze, Applications of Schur rings in algebraic combinatorics: graphs, partial difference sets and cyclotomic schemes, Dissertation, Oldenburg 2001.

[19] C.Hering, M.W. Liebeck and J. Saxl, The factorizations of the finite exceptional groups of Lie type, *J. Algebra* **106** (1987), 517–527.

[20] C. Jansen, K. Lux, R. Parker and R. Wilson, *An atlas of Brauer characters*, Oxford University Press, 1995.

[21] G.A. Jones, Cyclic regular subgroups of primitive permutation groups, *J. Group Theory*, **5** (2002), 403–407.

[22] L. K. Jorgensen, and M. Klin, Switching of edges in strongly regular graphs. I. A family of partial difference sets on 100 vertices, *Electron. J. Combin.* **10** (2003), Research Paper 17, 31 pp. (electronic).

[23] W.M. Kantor, k-homogeneous groups, *Math. Z.* **124** (1972), 261-265.

[24] P.B.Kleidman, The maximal subgroups of the finite 8-dimensional orthogonal groups $P\Omega_8^+(q)$ and of their automorphism groups, *J. Algebra* **110** (1987), 173-242.

[25] P.B. Kleidman and M.W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Series **129**, Cambridge University Press, Cambridge, 1990.

[26] A.S. Kleshchev and A.A. Premet, On second degree cohomology of symmetric and alternating groups, *Comm. Algebra* **21** (1993), 583–600.

[27] W. Knapp, On Burnside's method, *J. Algebra* **175** (1995), 644–660.

[28] C.H. Li, The finite primitive permutation groups containing an abelian regular subgroup, *Proc. London Math. Soc.* **87** (2003), 725–747.

[29] C.H. Li, Finite edge-transitive Cayley graphs and rotary Cayley maps, *Trans. Amer. Math. Soc.* **358** (2006), 4605–4635.

[30] C.H. Li and A. Seress, On vertex-transitive non-Cayley graphs of square-free order, *Designs, Codes and Cryptography* **34** (2005), 265–281.

[31] M.W. Liebeck, The affine permutation groups of rank three, *Proc. London Math. Soc.* **54** (1987), 477-516.

[32] M.W. Liebeck, C.E. Praeger and J. Saxl, Distance transitive graphs with symmetric or alternating automorphism group, *Bull. Austral. Math. Soc.* **35** (1987), 1-25.

[33] M.W. Liebeck, C.E. Praeger and J. Saxl, The maximal factorizations of the finite simple groups and their automorphism groups, *Mem. Amer. Math. Soc.* **86** (1990), no. 432.

[34] M.W. Liebeck, C.E. Praeger and J. Saxl, On factorizations of almost simple groups, *J. Algebra* **185** (1996), 409-419.

[35] M.W. Liebeck, C.E. Praeger and J. Saxl, Transitive subgroups of primitive permutation groups, *J. Algebra* **234** (2000), 291-361.

[36] P. W. Michor, Knit products of graded Lie algebras and groups, *Proceedings of the Winter School on Geometry and Physics, Srni, 1988*, Suppl. Rendiconti Circolo Matematico di Palermo, Ser. II, **22** (1989), 171-175. (ArXiv: math.GR/9204220)

[37] G. A. Miller, Groups Which are the Products of Two Permutable Proper Subgroups, *Proceedings of the National Academy of Sciences* **21** (1935), 469-472.

[38] B. H. Neumann, Decompositions of groups, *J. London Math. Soc.* **10** (1935), 3–6.

[39] B. H. Neumann, Commentary on Chapter 2, in *Selected works of B. H. Neumann and Hanna Neumann.* Editors: D. S. Meek and R. G. Stanton, Charles Babbage Research Centre, Winnipeg, Canada, 1988. Volume 1, pp. 65–67.

[40] C.E. Praeger, The inclusion problem for finite primitive permutation groups, *Proc. London Math. Soc.* **60** (1990), 68–88.

[41] J. Szep, On the structure of groups which can be represented as the product of two subgroups, *Acta Sci. Math. Szeged* **12** (1950), 57-61.

[42] G.E. Wall, On the conjugacy classes in the unitary, symplectic and orthogonal groups, *J. Austral. Math. Soc.* **3** (1965), 1-62.

[43] J. Wiegold and A.G. Williamson, The factorization of the alternating and symmetric groups, *Math. Z.* **175** (1980), 171-179.

[44] H. Wielandt, Finite Permutation Groups, Academic Press, New York-London 1964.

[45] S.J. Xu, X.G. Fang, J. Wang and M.Y. Xu, On cubic s-arc transitive Cayley graphs of finite simple groups, *European J. Combin.* **26** (2005), 133–143.

[46] G. Zappa, Sulla costruzione dei gruppi prodotto di due dati sottogruppi permutabili traloro, *Atti Secondo Congresso Un. Mat. Ital., Bologna, 1940*, Edizioni Cremonense, Rome, 1942, 119125.

[47] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math. Phys.* **3** (1892), 265–284.

Department of Mathematics, Imperial College, London SW7 2BZ, UK

School of Mathematics and Statistics, University of Western Australia, 35 Stirling Highway, Crawley, WA 6009, Australia

DPMMS, CMS, Wilberforce Road, Cambridge CB3 0WB, UK